Réseaux
Mr Quettier

Aurore Soors

Chapitre 1

Terminologie et modèles de référence

1.1 Définitions de base

Définition. *Un **réseau d'ordinateurs** est un ensemble d'ordinateurs autonomes interconnectés par une seule technologie.*

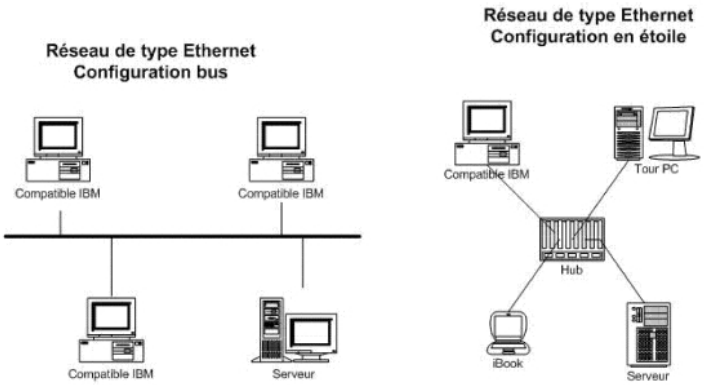
Définition. *Deux **ordinateurs** sont considérés comme interconnectés si ils sont capables d'échanger des informations.*

1.2 Les critères de classement des réseaux

1.2.1 La technique de transmission

Définition. *La technique de transmission est la manière dont les données sont envoyées d'un ordinateur vers un autre.*

1.2.1.1 La diffusion (Broadcast)

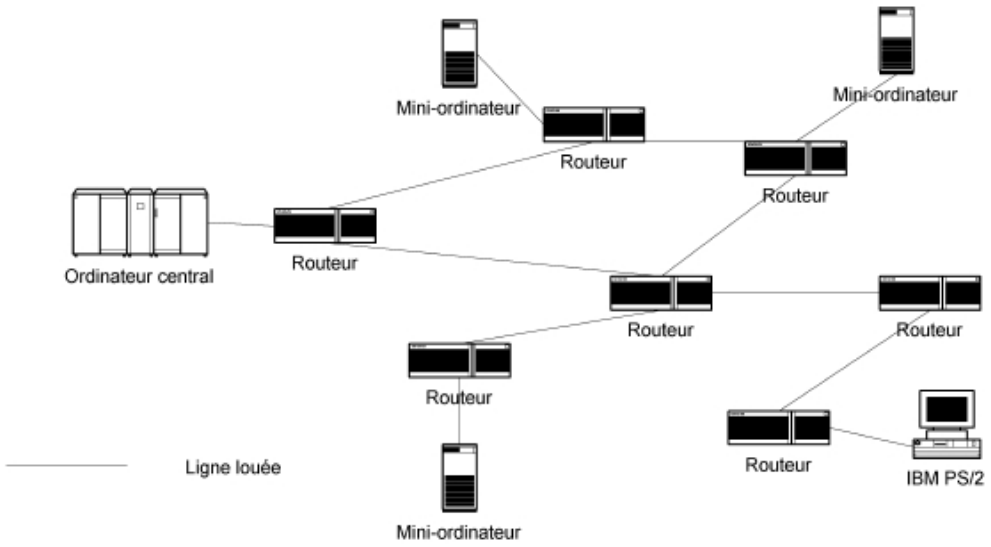


La trame utilisée est la suivante :

Adresse destination	Adresse source	Données

- Un seul canal de communication est partagé entre l'ensemble des machines
- Ce canal peut être un câble coaxial , un hub, un switch ou encore une fréquence radio.
- L'information est découpée en trames par la carte réseau. Une trame est une structure de données et le format de trame le plus rependu est ethernet.
- Toutes les cartes connectées peuvent recevoir la même trame.
- Adresse physique identifie la carte destinataire pour éviter l'ambiguïté. Dans les réseaux Ethernet, cette adresse dite physique porte le nom d'adresse MAC.
- Seul le destinataire traite la trame (recevoir <> traiter).

1.2.1.2 Les réseaux point à point



- Point à point, signifie que les machines sont reliées deux à deux par une paire torsadée ou fibre optique. Pour aller de la source à la destination, les informations vont passer par des machines intermédiaires appelées routeurs/commutateurs.
- Dans ce type de réseau, toutes les interfaces des machines (routeurs inclus) doivent avoir une adresse dite logique qui les identifie de manière unique. Sur internet, c'est l'adresse ip qui joue ce rôle.
- Toute transmission ne concerne que les deux machines situées aux extrémités. Contrairement aux techniques de diffusion, tout le monde ne reçoit pas la trame.
- Usage le plus fréquent : la connexion à Internet par modem classique.

Les principaux avantages de cette technologie est qu'on sait qui est à l'autre bout et qu'il y a une meilleur sécurité.
Il offre un débit plus lent (à cause de la technologie) mais l'avantage est qu'on va pouvoir parcourir de plus grandes distances et donc relier des sites géographiquement différents.

- Pour les besoins internes de leurs sites, les entreprises adoptent largement les techniques de type diffusion en raison de leur faible coût et la facilité de mise en œuvre de ces techniques.
- Pour les liaisons entre différents sites, par exemple des agences bancaires à leur site central, ce sont les technologies de type point à point qui sont privilégies car elles sont conçues pour cette optique.
- Internet s'est développé sur des lignes point à point et vu ses avantages tout le monde dans l'entreprise veut en bénéficier.
- Financièrement, il n'est pas possible d'offrir à chaque employé une connexion point à point

Nombre de cable pour n ordi = $(n * (n-1))/2$.

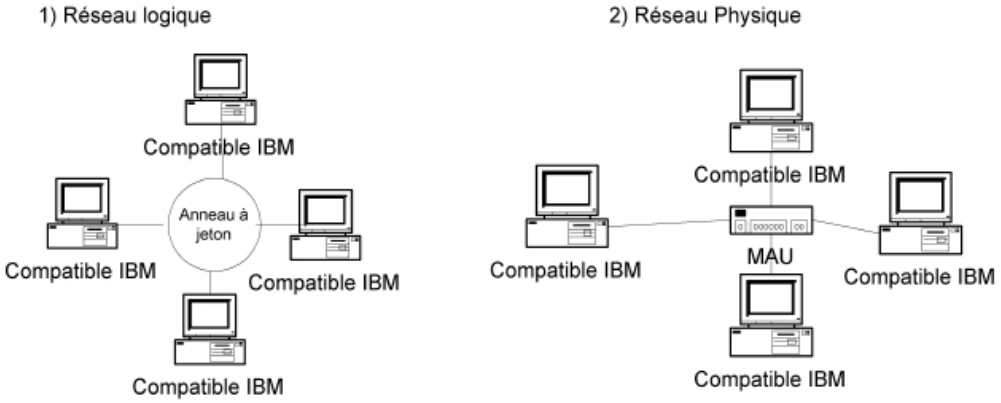
1.2.2 La taille du réseau

1.2.2.1 LAN (Local Area Network)

Définition :
- La taille se limite à quelques kilomètres avec débit de 10 mégabit/s à 10 gigabits/s. En principe le LAN est la propriété d'une seule organisation.
- Souvent c'est un système de type Diffusion. Certaines sources considèrent la variante Ethernet full-duplex comme point à point mais attention ce système utilise toujours des diffusions.
- trois types de topologies pour les câblages : Anneau, Bus, Etoile.

Topologies Bus et étoile (illustré plus haut) :
- Un câble linéaire pour les vieux systèmes et topologie en étoile pour les systèmes récents.
- Ethernet est la technologie de type bus la plus répandue.
- Dans les réseaux Ethernet, on rencontre également des topologies en étoile via un hub. Leur fonctionnement est identique à la topologie en bus.

Topologies en anneau :



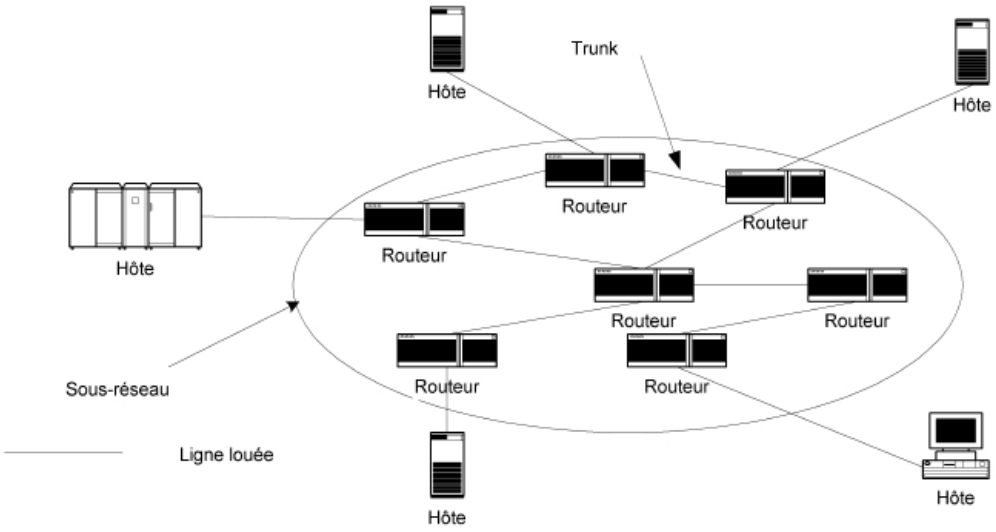
- Un câble (éventuellement doublé) relié en boucle.
- Le Token Ring d'IBM est le plus connu. Dans la même catégorie, citons FDDI.
- Un paquet spécial dit jeton, tourne en permanence.
- Seul celui qui prend possession du jeton peut émettre. Sur les systèmes de grande taille plusieurs jetons peuvent circuler.
- Il n'a cependant pas d'anneau apparent. L'anneau est contenu dans un coffret spécial appelé MAU (Media Acess Unit).
- Les technologies de type anneau existent encore dans les entreprises mais sont en voie d'abandon.

Un autre type est le FDDI : deux anneaux en fibre optique. Ce système est utilisé pour lier entre eux les serveurs et les disques durs.
Physiquement, le FDDI était physiquement une topologie en anneau tandis que token ring était une topologie en étoile.

1.2.3 MAN (Metropolitan Area Network)

Ces réseaux sont à l'échelle d'une ville et les technologie de type diffusion y règnent en maître. Exemple : VOO.

1.2.4 WAN (Wide Area Network)

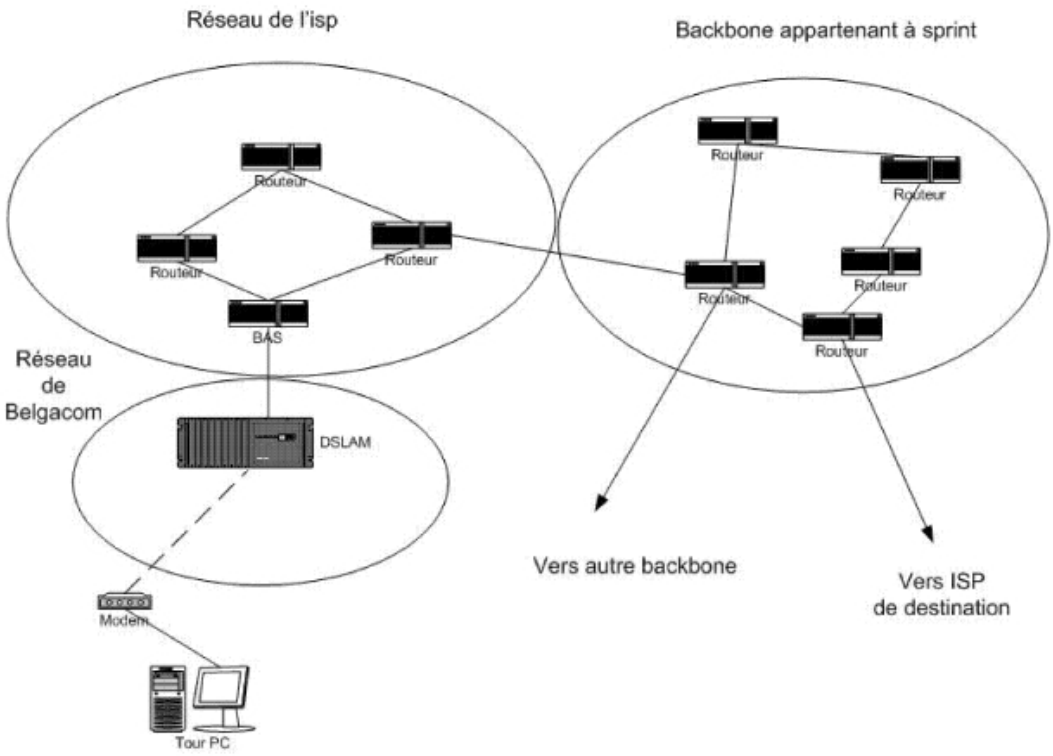


- Le réseau WAN est composé de Hôtes souvent connectés en réseau local et d'un sous-réseau.
- Chaque hôte dispose d'une adresse logique qui l'identifie de manière unique. Si les Hôtes sont connectés via un réseau local, seul le routeur doit disposer d'une adresse unique.
- Le sous-réseau de communication relie les hôtes et les réseaux locaux. Il est composé de routeurs qui disposent chacun d'une adresse logique. Le sous réseau véhicule les paquets entre les hôtes au moyen de trames.
- Les lignes de transmission sont appelées circuits, canaux (channel), ou faisceaux (trunks).
- Le fonctionnement d'un routeur est assimilable à un aiguillage. Au lieu d'aiguiller des wagons, on aiguille des paquets de données. On appelle cela le routage.
- Les paquets contiennent également les informations de routage sous la forme d'une adresse source et destination.
- Les paquets sont véhiculés par des trames entre deux paires de machines ou routeurs.
- Dans la plupart des WAN, les paquets sont transportés entre les routeurs selon une technologie point à point mais une technologie diffusion est possible aussi.
- Version simplifiée du routage est la commutation, qui sacrifie la souplesse au profit de la vitesse de traitement.

Trame	Paquet		
	Adresse source	Adresse destination	Données

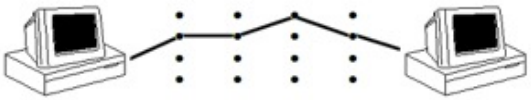
1.2.5 Internet

Internet est un réseau global constitué de réseaux distincts permettant aux ordinateurs de toute sorte de communiquer et partager des services directement et de manière transparente.



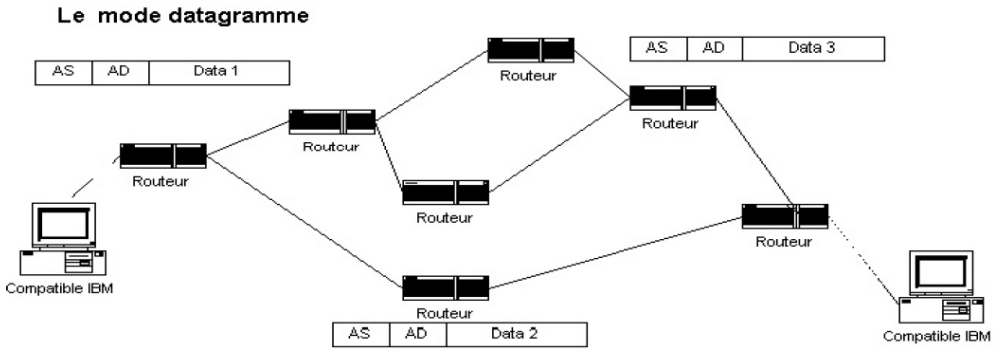
1.2.6 Le type de commutation

1.2.6.1 La commutation de circuit



- Le réseau téléphonique (non Gsm) est constitué des téléphones des abonnées et d'une série de commutateurs. Les commutateurs forment une hiérarchie.
- Quand une personne établit une communication avec une autre, un circuit physique est établi à l'intérieur des commutateurs le temps de la durée de la communication téléphonique.
- Autrefois les commutateurs étaient manuels et une opératrice avait une série de connecteurs correspondant aux téléphones des abonnés sur un tableau. Pour mettre en communication deux téléphones, elle reliait les connecteurs par un câble muni de deux fiches.
- Dans le cas d'un téléphone classique, l'usager quand il parle génère un signal électrique de tension variable.
- Le circuit est réservé pour la durée de la communication. Ceci explique la tarification à la durée, sachant que l'abonné à un usage exclusif du circuit.

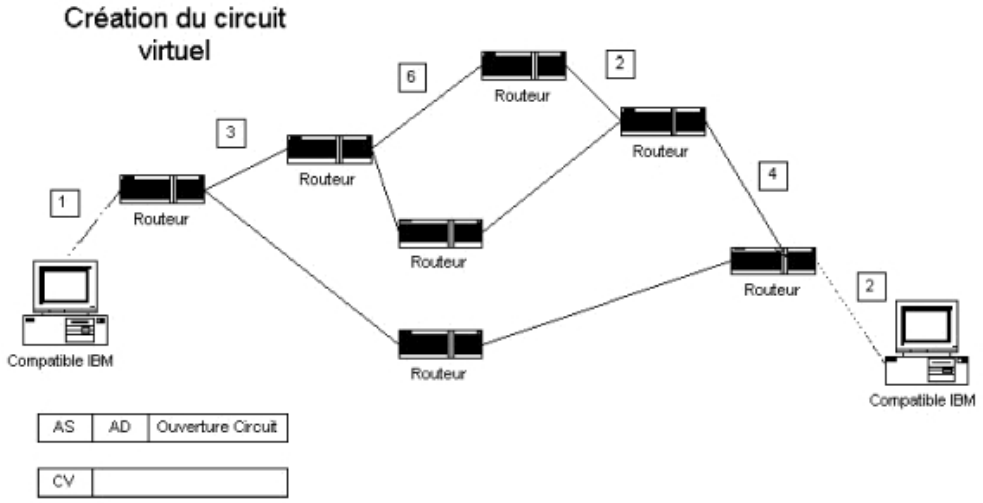
1.2.6.2 Le mode datagramme



où AS est l'adresse source, AD est l'adresse destinataire et Data2 les données à transmettre.

- Les lignes disposent de tampons en entrée et en sortie.
- Ces tampons peuvent contenir des paquets qui sont générés par les ordinateurs.
- Les paquets ont une taille fixe et c'est à charge des machines de découper l'information à l'envoi et la reconstituer à la réception.
- Le passage de l'information se fait en recopiant le paquet du tampon d'une ligne vers le tampon d'une autre ligne.
- Les réseaux datagrammes sont plus robustes que le circuit virtuel.
- Chaque paquet contient une adresse source et destination.
- L'adresse destination (adresse logique) sert au routeur à déterminer la ligne de sortie pour chaque paquet entrant.
- La décision est effectuée sur la base d'une table de routage qui indique pour chaque adresse la ligne de sortie à utiliser. Si le routeur ne trouve pas l'adresse, une entrée par défaut indique la ligne de sortie à utiliser.
- On notera que l'adresse destination n'est jamais modifiée contrairement au numéro de circuit virtuel.

1.2.6.3 Le mode virtuel



Un circuit est établit avant l'envoie des données. Le chemin choisit se fera en fonction de a source et de la destination.

- Un circuit est établi comme dans la commutation de circuit
- Il n'y a pas de circuit physique mais des tampons en entrée et en sortie.
- Pour établir le circuit, un paquet initial contenant une adresse source et une adresse destination sera expédié. Ce paquet détermina les lignes empruntées. Le but du routeur est de faire correspondre une ligne en entrée et en sortie.
- Chaque ligne se voie attribuer un numéro de circuit virtuel.
- Tout le trafic suivra la même route. Les paquets suivants utiliseront ce numéro de circuit virtuel
- A l'entrée de chaque routeur, ce numéro sera remplacé par le numéro à suivre en sortie. Les numéros successifs seront 1,3,6,2,4,2 pour notre exemple.

⇒ Utilisé pour le protocole ATM (exemple : ADSL).
D'où la facturation à la quantité de données.

1.3 Logigiel Réseau

1.3.1 Principe d'une architecture en couche

Dans un système d'exploitation, une architecture en couches est un ensemble de processus (programmes) qui communiquent entre eux, le processus de niveau supérieur utilisant les services de celui de niveau inférieur . Le noyau à la différence des autres processus restera toujours en mémoire, les autres processus peuvent se trouver sur le disque. Toute cette architecture repose évidemment sur le hardware.

APPLICATION
OS
BIOS
HARDWARE

Intérêt d'une architecture en couche : Offrir un maximum de modularité. On peut remplacer un module par un autre à condition qu'il respecte les mêmes services. L'objectif est aussi d'offrir un maximum d'indépendance vis-à-vis du matériel.

Concepts et avantages d'un modèle en couche :
- **Facilité de compréhension** : Une subdivision des fonctions permet de mieux décrire et apprendre les spécifications de protocoles.
- **Facilité de développement** : Une réduction de la complexité facilite la modification des programmes et accélère l'évolution des produits.
- **Inter-opérabilité entre fabricants** : Le fait de créer des produits qui se conforment à des normes communes permet aux ordinateurs et équipements de fabricants différents d'interagir au sein d'un même réseau
- **Ingénierie modulaire** : Un fabricant peut écrire un logiciel qui implémente les fonctions de couches supérieures (par exemple, un navigateur web) pendant qu'un autre écrit un logiciel qui implémente celles de couches inférieures (Par exemple, les services TCP/IP intégrés par Microsoft dans ses systèmes d'exploitation.

1.3.2 Hiérarchies de protocoles

Protocoles		Services
Directeur général	$\Longleftrightarrow$	Directeur général
Secrétaire	$\Longleftrightarrow$	Secrétaire
Poste	$\Longleftrightarrow$	Poste

Définition. *Un **service** est un ensemble de primitives (opérations) qu'une couche fournit à la couche immédiatement supérieure. Le service définit les opérations que la couche est prête à effectuer pour le compte de ses utilisateurs.*

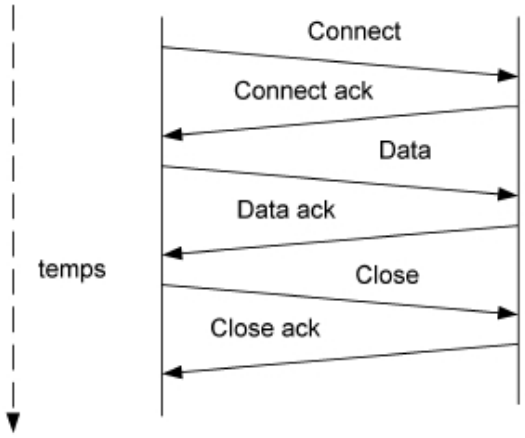
Définition. *Un **protocole** est un ensemble de règles s'appliquant au format et à la signification des trames, paquets ou messages échangés entre entités paires au sein d'une couche. Les entités utilisent les protocoles pour implémenter leurs spécifications de services.*

Analogie avec la poste : la poste vous offre la possibilité d'envoyer des colis. C'est un service. Elle peut pour livrer, utiliser des motos, camionnettes ou avions. Les protocoles sont les moyens de transport.

1.3.3 Protocoles/services en mode connecté/déconnecté

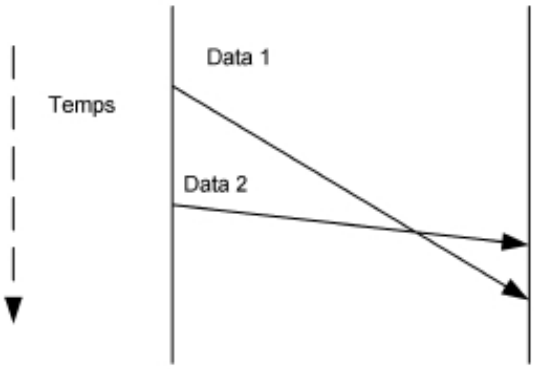
Chaque couche peut utiliser un protocole en mode connecté ou non-connecté. Dans une pile de protocoles, les couches peuvent soit en mode connecté ou non connecté.

1.3.3.1 Protocole en mode connexion



- Une connexion est établie au préalable avant délivrance des paquets d'information.
- Elle est supprimée quand les paquets d'information sont délivrés.
- L'ordre de délivrance est respecté et chaque donnée est numérotée.
- La fiabilité est garantie via un mécanisme d'acquittement (ack = acknowledge)
- L'ouverture d'une connexion est pénalisante en temps.
- L'avantage d'un mode connecté, est que l'on prévient le récepteur qu'il va recevoir des données et il peut prendre ses dispositions pour éviter les pertes. Ce système permet aussi au récepteur de refuser les connexions pour lesquelles il n'a pas les ressources garanties.
- Le téléphone est l'exemple classique du protocole en mode connecté.

1.3.3.2 Protocole déconnecté ou sans connexion



- On délivre directement l'information.
- Chaque message est acheminé de manière indépendante.
- L'ordre de délivrance des messages n'est pas garantit.
- La fiabilité n'est garantie car vous n'avez aucune garantie que le récepteur soit à l'écoute de vos informations et parce qu'il n'y a pas de mécanisme d'acquittement.
- Dans certains cas, le fait qu'un protocole en mode non connecté soit performant prime sur le fait qu'il soit fiable.
- Les drivers des cartes réseaux ethernet, token ring et fddi travaillent en mode non connecté.
- Le streaming est l'exemple type du protocole déconnecté.

1.4 Les modèles et normes de référence

Il existe actuellement trois architectures en couches dans le monde. Elles sont les suivantes :

Modèle	Concrètement	Situation technologique
OSI	Rien	Passé
TCP/IP	Réseaux locaux, Connexion Modem	Présent
ATM	Connexion ADSL	Le standard pour les connexions ADSL

1.4.1 Le modèle de référence OSI (Open System Interface)

Ce modèle est né d'une proposition élaborée par l'Organisation internationale de normalisation (ISO).Il est appelé Modèle de Référence OSI (Open System Interconnection) parce qu'il traite de la connexion entre système ouverts à la communication avec d'autres systèmes (dits systèmes ouverts). Il est appelé plus communément modèle OSI et il a été définit avec 7 couches.

Numéro	Nom de la couche	Description
7	Applications	Services applicatifs
6	Présentation	Présentation, représentation des données
5	Session	Service de session : vérification, gestion
4	Transport	Vérification de l'intégrité des données Multiplexage par-dessus une connexion réseau
3	Réseaux	Routage des données
2	Liaison des données	Transmission de l'information en paquet de bits
1	Physique	Transmission du courant de bits au dessus du support physique

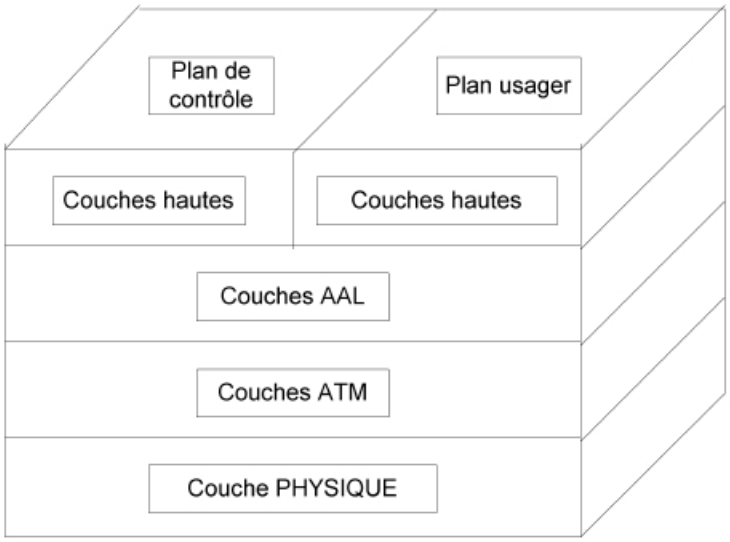
Ce modèle a l'avantage d'être relativement complet et de prendre en charge tous les problèmes que l'on peut rencontrer dans le domaine des télécommunications. Malheureusement sa complexité engendre notamment trop de redondances au niveau de la gestion des erreurs et l'oubli de problèmes aussi essentiels que la sécurité ou l'administration réseau font que les implémentations de ce modèle sont restées relativement confidentielles et quand il y'a eut implémentation, cela n'a jamais concerné l'ensemble des couches.

1.4.2 Le modèle TCP/IP

TCP = Transfert Control Protocol et IP = Internet Protocol
Le modèle TCP/IP paraît plus simple car il a deux couches en moins mais les couches sessions et présentations sont gérées par les applications.

1.4.3 Le modèle ATM

Avec ATM, un nouveau modèle de télécommunication est apparu. Ce modèle est distinct du modèle OSI (qui est resté essentiellement un modèle théorique) comme l'était déjà le modèle TCP/IP. Le modèle ATM est en fait un modèle tridimensionnel contrairement aux autres modèles. ATM est une architecture en mode connecté de type circuit virtuel.



Le modèle ATM est divisé en plans qui sont eux-mêmes divisés en couches.
- Le plan usager qui traite des fonctions de transport de données, de contrôle de flux, de corrections d'erreurs et autres.
- Le plan de contrôle traite de la gestion de la connexion (établissement de cette dernière).

Chapitre 2

La couche physique : les signaux, cablages et interfaces

2.1 Couche physique

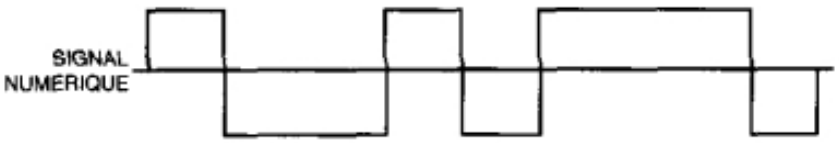
– La couche physique concerne le support de transmission ainsi que la nature des signaux.
– Les canaux sont répartis en deux catégories : les canaux numériques et les canaux analogiques.

2.2 Distinction entre la transmission analogique et digitale

2.2.1 La transmission analogique

Définition. *Un **signal analogique** est un signal qui varie de manière continue dans le temps. Il ne peut avoir de coupures ou de discontinuités. Une onde périodique répond parfaitement à ces critères. Cette onde se caractérise par une amplitude et une fréquence. Pour transmettre des informations, on va appliquer des transformations à cette onde. C'est ce qu'on appelle la modulation. Cette fonction sera appliquée par un modem.*
*Les **supports de transmissions analogiques** sont : la fibre optique, le câble coaxial de télédistribution, la ligne adsl, ...*
*Il **se caractérise** donc par :*
– *Aucune discontinuité*
– *N'importe quelle valeur*
– *Peut changer n'importe quand*

2.2.2 La transmission digitale ou numérique



Définition. *Dans un **signal digital**, le signal maintient un certain niveau pendant une certaine période puis passe brusquement à un autre niveau.*
*Les **supports de transmissions numériques** sont : le bus d'ordinateur, le câble série, la norme ethernet, la norme RNIS, ...*
*Il **se caractérise** donc par :*
- *Discontinu*
- *Prend quelques valeurs prédéfinies*
- *Maintient une valeur pendant un certain temps (durée prédéfinie)*

2.2.3 Conversion des signaux

Données	Appareil	Signal
Anaogique	Téléphone∗	Analogique
Analogique	Codec∗∗	Numérique
Numérique	Transmetteur	Numérique
Numérique	Modem∗	Analogique

∗ : Les plus utilisés de nos jours.
∗∗ : Utilisé chez les opérateurs de TéléCom.

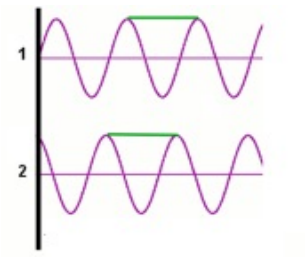
2.3 Bases théoriques de la transmission de données

2.3.1 Représentation du courant électrique (d'un signal périodique)

Les informations sont transmises sur des supports de transmission en faisant varier certains paramètres physiques des signaux qui les représentent, par exemple, la tension électrique.
Le courant électrique peut être représenté par plusieurs fonctions sinus ou cosinus.

$$Signal(t) = A* \sin(t + D)$$

Où :



- A est l'amplitude
- f la fréquence (f = 1/T où T est la période
(représentée en vert ci-contre)
- t le temps
- D le déphasage exprimé en radians
(est le retard pris au démarrage (ci-contre, 2 est déphasé))

2.3.2 Décomposition en série de Fourrier

Définition. *Toute fonction périodique g(t), ayant pour période T, peut être décomposée en une somme (peut être infinies) de fonctions sinus ou cosinus.*
Autrement dit, tout signal périodique peut être décomposé en une somme de sinusoïdes.

$$G(t) = \tfrac{1}{2}C + \sum_{n=1}^{\infty} a_n \sin(2.\Pi.n.f.t) + \sum_{n=1}^{\infty} b_n \sin(2.\Pi.n.f.t)$$

En théorie, tout câblage électrique doit pouvoir faire passer un signal électrique. Malheureusement, les supports électriques sont limités par leur bande passante exprimée en hertz et toute harmonique qui a une fréquence supérieure est sérieusement perturbée. Ceci se traduira par une dégradation du signal.

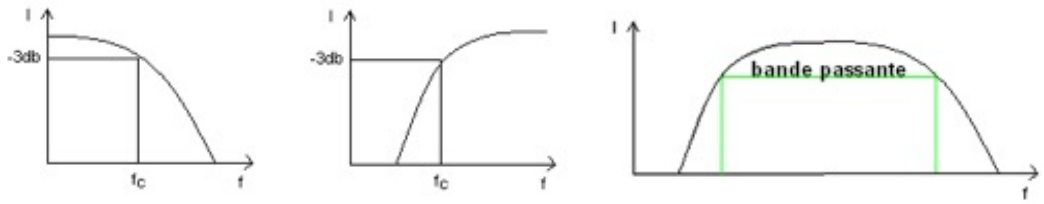
2.3.3 La définition du décibel

Le bruit sur un canal est exprimé par le rapport signal sur bruit (rapport des puissances), en anglais S/N (Signal to Noise). Toutefois, dans l'industrie, on préfère employer le terme décibel.

$$Bel = \log_{10} \frac{P_1}{P_2}$$
$$Decibel = 10 \log_{10} \frac{S}{N} = \log_{10} \frac{P_1}{P_2}$$

2.3.4 Définition de la bande passante et de la fréquence de coupure

- Aucun système de transmission n'est en mesure d'émettre des signaux sans leur faire subir d'affaiblissement. Cet affaiblissement est exprimé en décibel/km.
- Tous les composants harmoniques ne subissent pas la même déformation (distorsions).
- Notion de fréquence de coupure (fc) exprimée en hertz. Toute fréquence de coupure supérieure à fc subit une forte atténuation.
- Toute les harmoniques qui dépassent la fréquence de coupure sont perdues et plus la fréquence de coupure est basse, plus le nombre d'harmoniques disponibles sera réduis, ce qui dénature le signal.
- Bande Passante (bandwith) = espace de fréquence transmit avec un affaiblissement acceptable, exprimé en hertz.
- Pour une bande passante correcte, l'affaiblissement toléré est de 3db (ci-dessous : à gauche le filtre passe bas et à droite le filtre passe haute).



2.3.5 Influence du débit sur la transmission des harmoniques

On ne peut envoyer un signal à trop grande vitesse car il y a un risque de ne pas recevoir le signal en sortir car il y a trop peu d'harmoniques.
Exemple :

F1 =	500hz	F2 =	1000hz
	1000hz		2000hz
	1500hz		3000hz ∗
	2000hz		
	2500hz		
	3000hz		

∗ Je risque de ne pas avoir un bon signal, fidèle à celui émis.

2.3.6 Débit maximum théorique d'un canal de transmission

Nyquist a montré que si un signa quelconque était appliqué à l'entrée d'un filtre passe-basse ayant une bande passante H, le signal pouvait être reconstitué à partir d'un échantillonnage selon une cadence de $2H$ par seconde.
Si le signal comporte un nombre V de niveaux significatifs, le théorème conduit à la formule :

$$D_{max} = 2.H.\log_2 V$$

Si la bande passante vaut 3000hz (ligne téléphonique) et qu'un codage à deux niveaux est employé. Un signal de 6000 bits/seconde peut être transmis.
Pour définir le nombre de signaux transmis par seconde, le terme **baud** est utilisé.

Définition. *Un **Baud** est le nombre de changement d'état par seconde du signal ou encore, nombre de symboles transmis par seconde.*

Dans l'exemple précédent, le nombre de bauds est de 3000 et le nombre de bits transmis est de 6000.
Plus on augmente le nombre de niveaux de signaux, plus la quantité d'information transmise doit augmenter. C'est cette technique qu'utilisent les modems.

2.3.7 Débit maximum pratique d'un canal de transmission

Malheureusement, les canaux de transmission sont soumis à des bruits divers. Ce sont ces bruits qui vont imposer une limite au nombre de niveau du signal car plus le nombre de niveau augmente plus il est difficile de les discerner.

Théorème. *Le théorème de Shannon montre que, pour un canal de transmission de bande H soumis à un rapport signal sur bruit de S/N, la capacité de transmission maximale C, en bit/seconde, est donnée par*

$$C = H.\log_2(1 + \tfrac{S}{N})$$

Si la bande passante est de 3000hz et un rapport $\frac{S}{N}$ de 1000, doit 30db (valeur typique pour le réseau téléphonique analogique), on obtient une valeur de C = 30.000 bit/seconde, quel que soit le nombre de valeurs représentatives du signa et la fréquence d'échantillonnage utilisée.

2.4 Les modems

2.4.1 Le principe

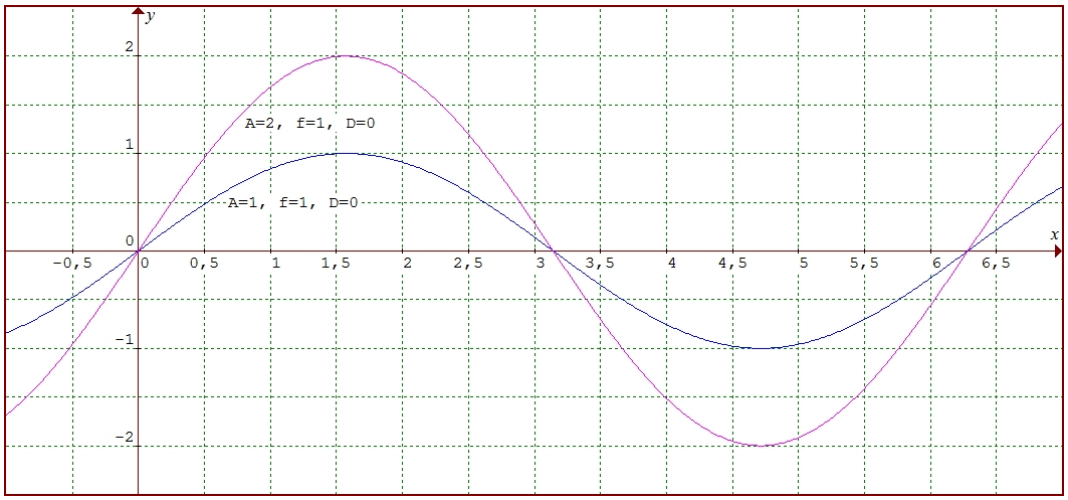
- Les signaux rectangulaires (digitaux) sont soumis à de fortes atténuations et distorsions lorsqu'ils sont transmis sur un média à faible bande passante.
- Transmission d'un signal sinusoïdal appelé signal porteur dont la fréquence est à l'intérieur de la bande passante.
- Pour transmettre l'information, on module l'amplitude, la fréquence ou la phase.
- L'équipement qui réalise l'opération est appelé un modem modulateur-démodulateur.

2.4.2 Les techniques de modulation

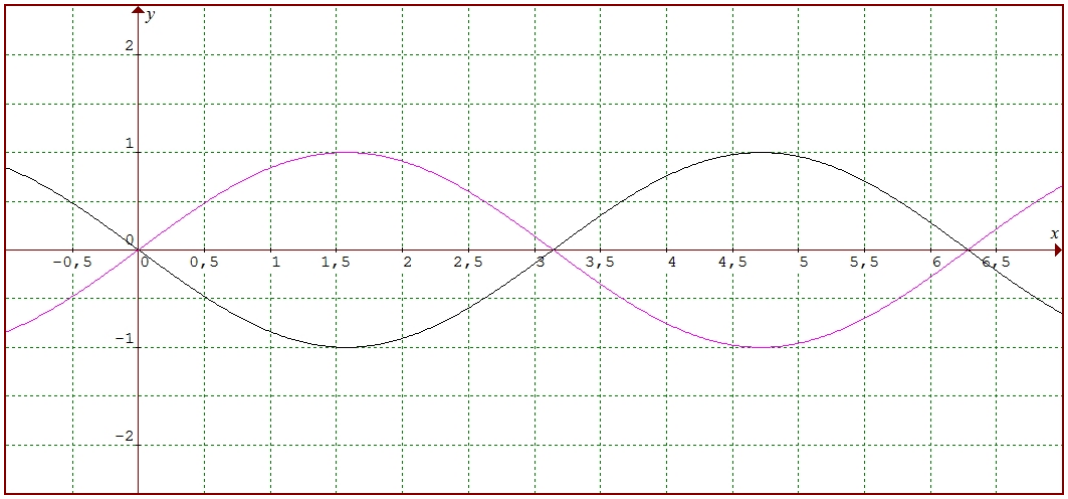
2.4.2.1 Représentation d'un signal électrique

$Signal(t) = A* \sin(t + D)$

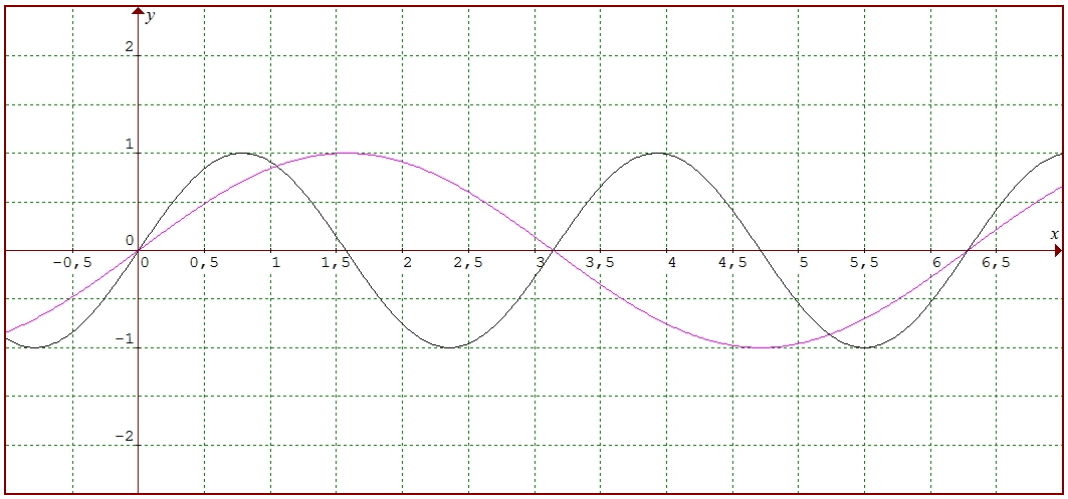
Modulation d'amplitude : Si l'amplitude devient trop petite, le signal devient difficilement discernable.



Modulation de phase :

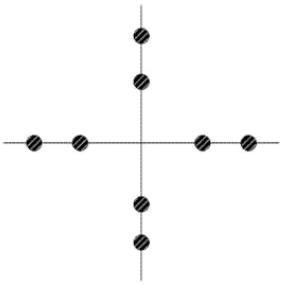


Modulation de fréquence :



2.4.2.2 Constellation diagramme

La constellation diagramme montre pour un codage donné les différentes combinaisons de modulation de phase et d'amplitude qu'un modem peut appliquer pour coder l'information.



Le plus simple, quatre niveau de phase et deux niveaux d'amplitude par phase (les deux points sur chaque segment) $\rightarrow$ 8 combinaisons ; $8 = 23 \rightarrow 3$ bits sont transmis par baud.

2.5 Les médias de transmission

2.5.1 Le câble électrique à paires torsadées

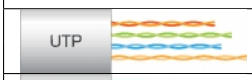
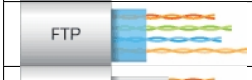
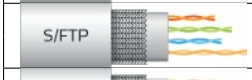
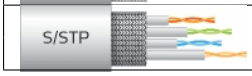
- C'est le plus ancien média de transmission.
- La paire torsadée (twisted pair) est composée de deux câbles en cuivre de 1mm de diamètre isolés et enroulée de façon hélicoïdale comme une molécule d'ADN (réduire les parasites).
- Les câbles dit de catégorie 3 et de catégorie 5 sont utilisés par les réseaux d'ordinateurs (Unshielded Twisted Pair = UTP).
- Les câbles de catégorie 3 sont constitués de 4 paires faiblement torsadées et recouvertes d'une gaine protectrice. Le débit autorisé est de 10 mégabit/s.
- Les câbles de catégorie 5 utilise un pas plus serré et un meilleur isolant (le téflon) et permet des débits de 100 mégabit/s avec 2 paires.

Pourquoi torsader les fils ? Parce que quand une boucle de courant est mise dans un champ magnétique variable, il y a production d'un courant électrique induit. Le fait de torsader les câbles permet de réduire le courant induit puisqu'on réduit la surface. C'est une protection contre les ondes parasitaires.

Types de paires torsadées :

Catégorie	Débit théorique	Usage
1	1 Mbps	Téléphone
3	10 Mbps	Ethernet 10 Mbps
5	100 Mbps	Ethernet 100 Mbps
5 enhanced	2000 Mbps	Gigabit Ethernet, Full duplex

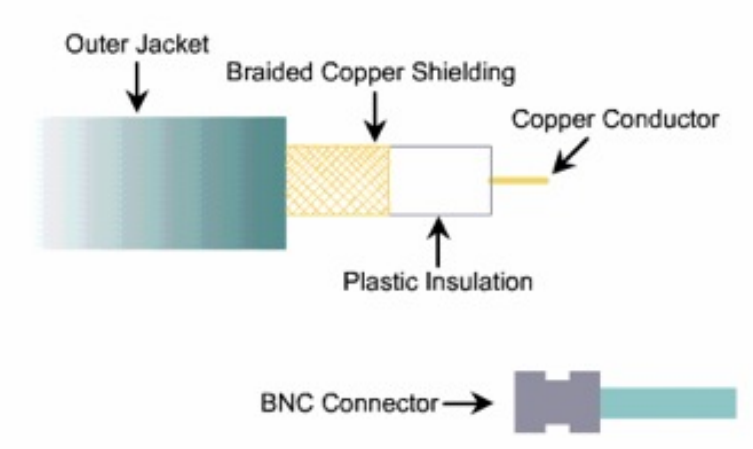
Types de blindage :

Illustration	Nom du blindage	Caractéristiques
	UTP	Le câble UTP (Unshielded Twisted Pair) est un câble non blindé, non écranté.
	FTP	Le câble FTP (Foiled Twisted Pair) est un câble écranté avec une feuille d'aluminium.
	STP	Le câble STP (Shielded Twisted Pair) est un câble écranté paire par paire.
	S-FTP	Le câble SFTP (Shielded Foiled Twisted Pair) est un câble écranté paire par paire et blindé.
	S-STP	Le câble SSTP (Shielded and Shielded Twisted Pair) est un câble blindé paire par paire avec un blindage autour.

Définition. ***Écranté*** *: Qualifie un câble où un feuillard de métal est enroulé autour des conducteurs pour assurer une protection contre les hautes fréquences parasites. Le câble écranté offre une meilleure immunité au bruit électronique.*

L'avantage du câble STP est qu'il a une meilleur isolation face aux ondes électromagnétiques et qu'il est plus rigide cependant il est plus cher et plus lourd.

2.5.2 Le câble coaxial bande de base



- Le câble coaxial est constitué d'un conducteur central rigide en cuivre, le cœur, entouré d'un matériel isolant de forme cylindrique enveloppée d'une tresse conductrice en cuivre, le tout recouvert de plastique.
- Excellente immunité contre les bruits ou perturbations électromagnétiques
- Seule une trame peut circuler à la fois. Si deux trames sont transmises simultanément, une collision se produit.
- Il existe en deux tailles : le thick (10 base 5) et le thin (10 base 2).
- Les deux types de câblage doivent impérativement se terminer par un Terminateur ou bouchon.

Type de câblage	Longueur segment	Nombre max. de connexions par segments
10 base 5	500 mètres	100
10 base 2	200 mètres	30

Explication du nom du type de câblage : si par exemple, on prend 10 base 2 cela veut dire que l'on aura un débit de 10 Mbps, la base peut être soit numérique (base brand) soit analogique (broad band) et le 2 permet d'identifier la longueur du câble ou le type de câble (par exemple TX pour Twisted, FX pour la fibre optique, ...).

2.5.3 La fibre optique

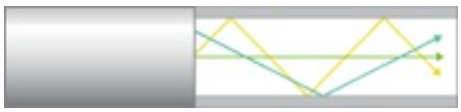
Sa structure
- La fibre est constituée de verre cylindrique appelé cœur.
- Ce cœur est entouré d'une deuxième couche concentrique, formée d'un verre spécial, mais dont l'indice de réfraction est inférieur à celui du cœur.
- Les couches des protections en matériaux divers.

La manière de véhiculer l'information
- L'information est transmise sous forme d'impulsions de lumière.
- La lumière se propage dans la fibre par réflexion le long des parois.
- Un ou plusieurs rayons peuvent se propager (multi ou mono).
- L'émetteur est une LED (Light-Emitting Diode) ou une LD (diode laser).
- Le récepteur est un photodétecteur qui est constitué d'une diode PIN ou d'une photodiode à avalanche.

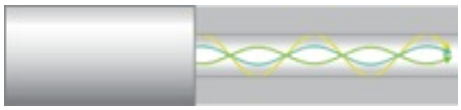
Les types de fibres optiques

- **Mono mode** : composée d'un coeur optique inférieur à 10 microns et d'une gaine de 125 microns. Sa bande passante est supérieure à 10 GHz/km ; elle est donc essentiellement utilisée pour les très longues distances.

- **Multi mode à saut d'indice** : constituée d'un coeur de 62,5 microns et d'une gaine optique de 125 microns, avec différents indices de réfraction. La section importante du coeur provoque une grande dispersion du signal et donc une dégradation des performances sur de très longues distances. Sa bande passante se situe entre 600 et 3000 MHz par km.



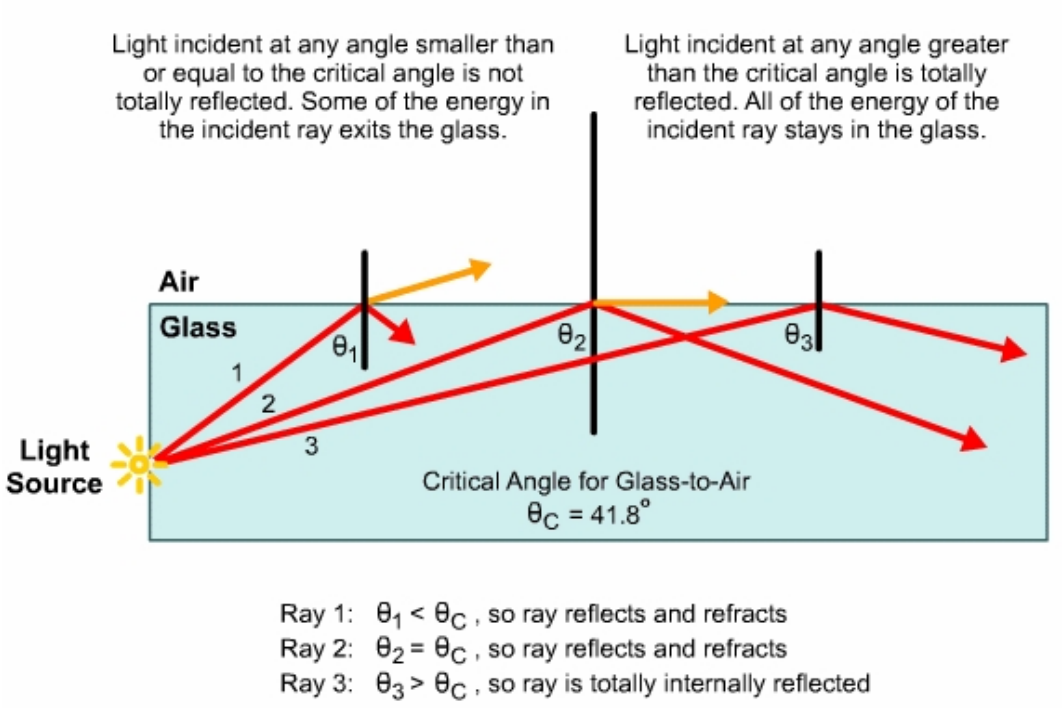
- **Multi mode à gradient** : le diamètre de son coeur est plus petit et est constitué de couches de verre successives ayant un indice de réfraction proche. Cela permet de réduire les problèmes posés par la dispersion du signal.



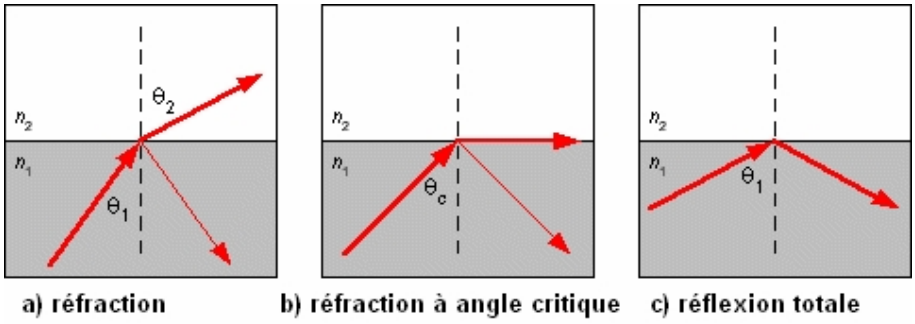
La fibre multimode
- Plusieurs rayons se transmettent simultanément. Comme le second rayon lumineux émit peut passer avant le premier vu qu'ils empruntent des chemins différents, cela limite la vitesse de transmission.
- Les fibres multi mode sont composées de deux catégories : on distingue les fibres à faible indice ou saut d'indice (débit limité à 50 Mb/s) et les fibres à gradient d'indice (débit limité à 1 Gb/s).
- Utilisation privée.

La fibre monomode
- Les vitesses atteintes sont de plusieurs Gb/s.
- La propagation du signal est axiale. Il n'y a plus de distorsion intermodale et la bande passante est accrue.
- Utilisation publique.

Propagation de la lumière dans la fibre optique



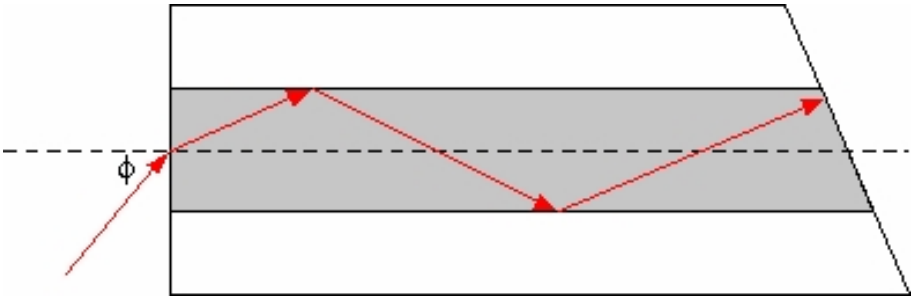
Le principe de la réflexion totale interne est à la base de la propagation des ondes lumineuses dans la fibre optique. D'après ce principe, lorsqu'un rayon lumineux passe d'un milieu à un autre dont l'indice de réfraction est plus faible, il peut être réfléchi. De plus, lorsque l'angle d'incidence du rayon lumineux est plus grand que l'angle critique, la lumière est réfléchie en totalité et il n'y a aucune perte de lumière.



La réflexion totale interne est régie par deux facteurs : les indices de réfraction des deux milieux et l'angle critique. Ces facteurs sont reliés par l'équation suivante :

$$\sin\theta = \frac{n_2}{n_1}$$

Lorsqu'un rayon lumineux entre dans une fibre optique à l'une de ses extrémités avec un angle adéquat, il subit de multiples réflexions totales internes. Ce rayon se propage alors jusqu'à l'autre extrémité de la fibre sans perte, en empruntant un parcours en zigzag.



Les avantages la fibre optique :

- Insensibilité aux phénomènes électroniques, à la foudre.
- Chimiquement neutre (un objet métallique peut être sujet à la corrosion).
- Atténuation très réduite permettant des applications « longue distance ».
- Large bande passante.
- Absence d'induction mutuelle (crosstalk).
- Faible poids et dimensions réduites.

Les inconvénients la fibre optique :

- Le coût plus élevé des médias ainsi que l'interface réseau.
- Difficulté de réaliser des connexions. Pertes relativement importantes en cas de connexions mécaniques. Il faut un équipement spécialisé.

Les facteurs limitant la distance :

- Le Power Budget ou Budget Optique : c'est l'atténuation maximale que peut subir le signa lors de sa propagation. Elle est exprimée en dB.
- L'atténuation linéique : c'est l'atténuation engendrée par la fibre et qui est fonction de sa longueur d'onde ; exprimée en dB/km.
- Les soudures et connexions : qui engendrent des pertes. Exemple : connexion de deux fibres optiques de genre différent (figure 1) ou lors de la soudure, il y a toujours des pertes (figure 2).
- La qualité de la source : la diode laser LD, grâce à sons spectre d'émission étroit, présente moins de distorsion du signal à la réception par rapport à la diode classique LED. Cela se traduit par un gain substantiel en dB au niveau du budget optique.

$$distance = \frac{BudgetOptique - PertesSoudures - PertesConnexions}{AttenuationLineique}$$

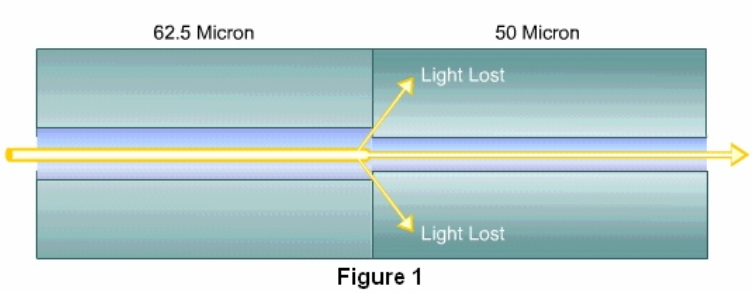
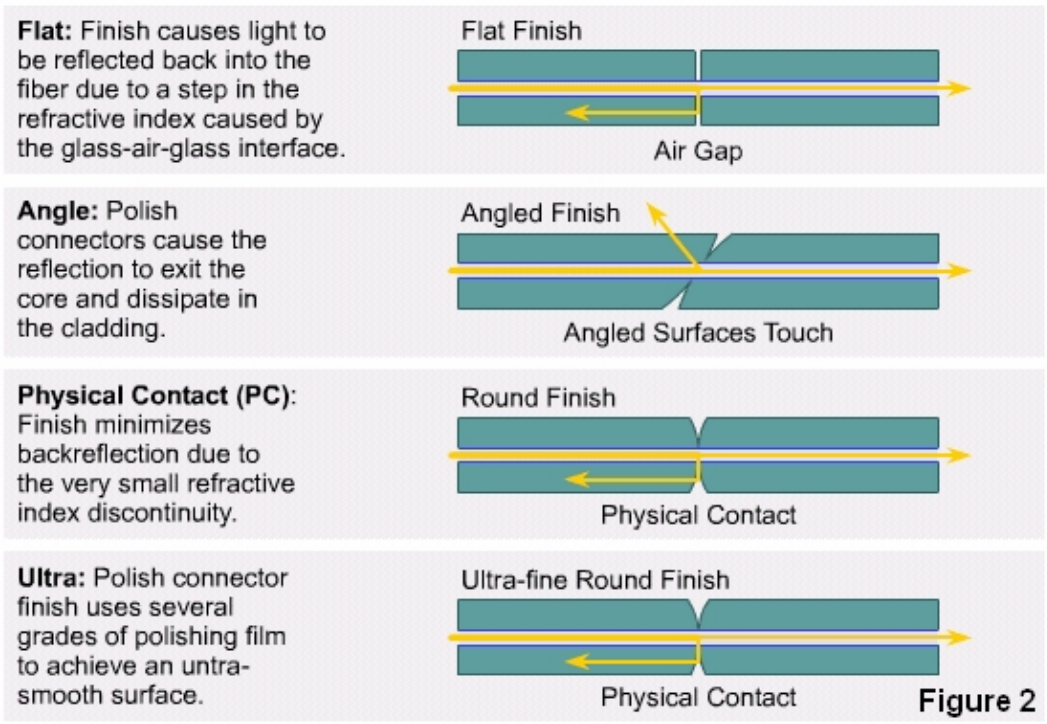
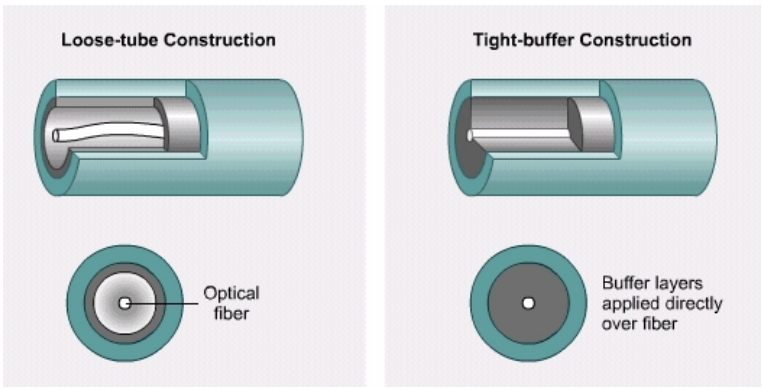


Figure 1


Flat: Finish causes light to be reflected back into the fiber due to a step in the refractive index caused by the glass-air-glass interface.
Flat Finish
Air Gap
Angle: Polish connectors cause the reflection to exit the core and dissipate in the cladding.
Angled Finish
Angled Surfaces Touch
Physical Contact (PC): Finish minimizes backreflection due to the very small refractive index discontinuity.
Round Finish
Physical Contact
Ultra: Polish connector finish uses several grades of polishing film to achieve an untra-smooth surface.
Ultra-fine Round Finish
Physical Contact
Figure 2

Gaine de protection :



- Loose Tube ou gaine lâche :
  - La fibre peut bouger dans le câble
  - Découple l'effort localisé
  - Empêche les petites courbures
  - Diminue l'atténuation
- Tight Buffer ou gaine étroite :
  - La fibre est fixe dans le câble
  - Haute résistance aux chocs
  - Résistante à l'usure
  - Petite taille

L'avantage d'une gaine lâche est que même si la fibre est pliée, la lumière continue sa trajectoire.

Influence de la courbure :

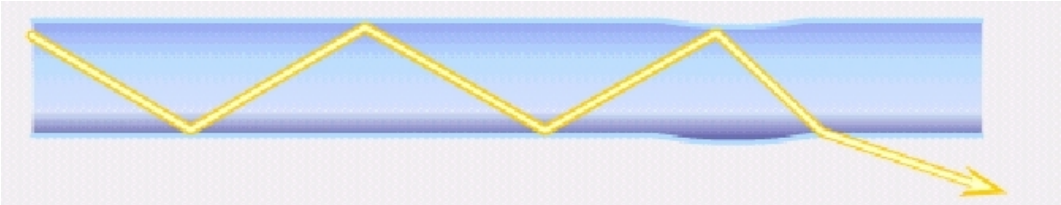


FIG. 2.1 – Faible courbure

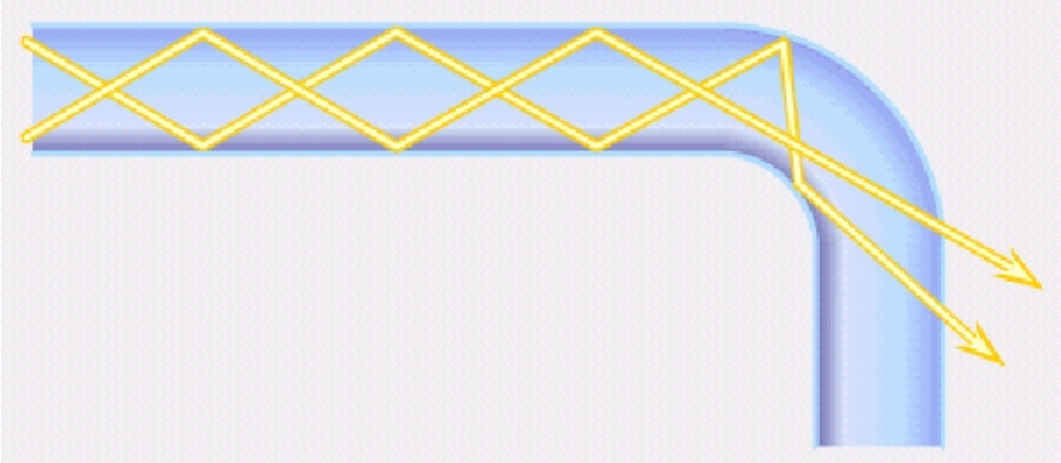
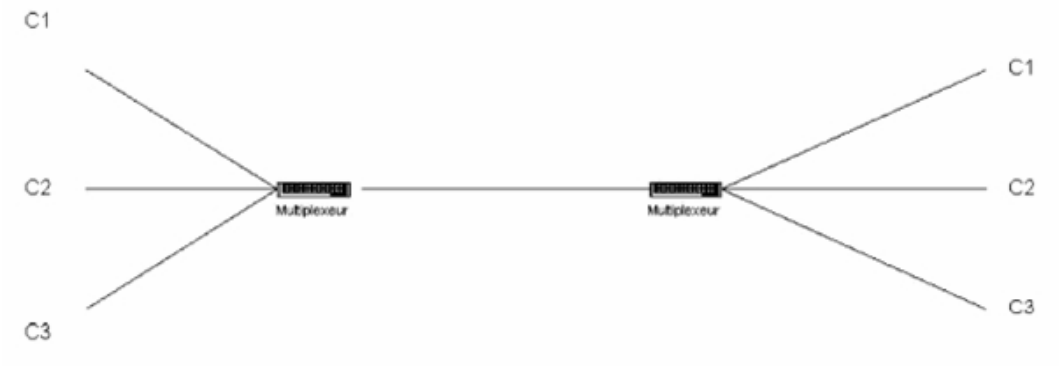


FIG. 2.2 – Courbure prononcée

2.6 Le multiplexage

2.6.1 Le principe du multiplexage



Dans un multiplexeur, il y a n entrées. Le multiplexeur est connecté par un simple lien vers un démultiplexeur. Le lien est capable de transporter n canaux séparés de données.
Le **multiplexeur** combine (multiplexe) les données à partir de n lignes d'entrées et les transmet vers une ligne de plus grande capacité.
Le **démultiplexeur** accepte le flux de données multiplexée, sépare (demultiplexe) les données fournies au canal, et délivre ces dernières aux n lignes appropriées.

Deux raisons expliquent l'efficacité du multiplexage :

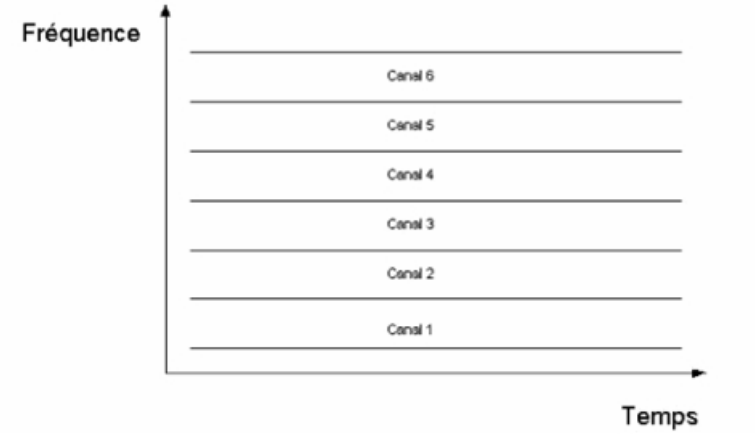
- Plus le débit est élevé, meilleur sera le rapport qualité/prix de la ligne de transmission.
- Pour une transmission efficace, on devra combiner plusieurs lignes à faible débit sur une ligne pour atteindre le plus haut débit possible. C'est justement ce que fait le multiplexage.

Il existe deux catégories de multiplexage :

- Le multiplexage temporel
- Le multiplexage fréquentiel

2.6.2 Le multiplexage fréquentiel

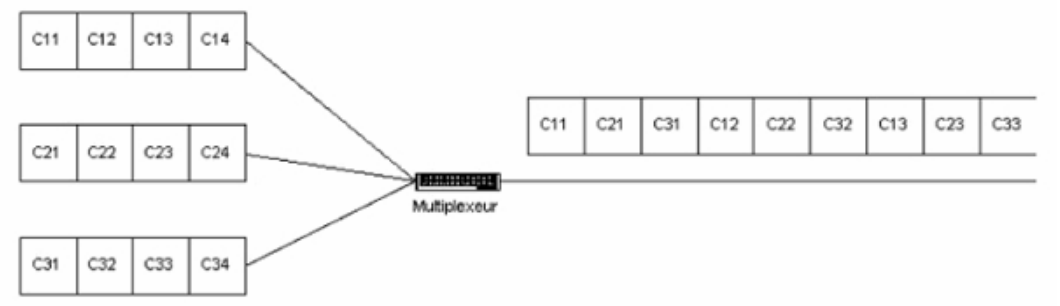
Définition. *Le **multiplexage fréquentiel** consiste à partager la bande de fréquences disponible en un certain nombre de canaux (ou sous bande) plus étroits et à affecter en permanence chacun de ces canaux à un utilisateur exclusif.*



Principe :
Le multiplexage fréquentiel est une technique où plusieurs signaux peuvent être transmis simultanément si chaque signal est modulé sur une fréquence porteuse différente et que les signaux des fréquences porteuses soient suffisamment séparés pour que les bandes passantes de ces signaux ne se recouvrent pas.

2.6.3 Le multiplexage temporel

Définition. *Le **multiplexage temporel** consiste à affecter à chaque utilisateur, pendant un court instant et à tour de rôle la totalité de la bande passante disponible.*



Il existe deux types de multiplexage :

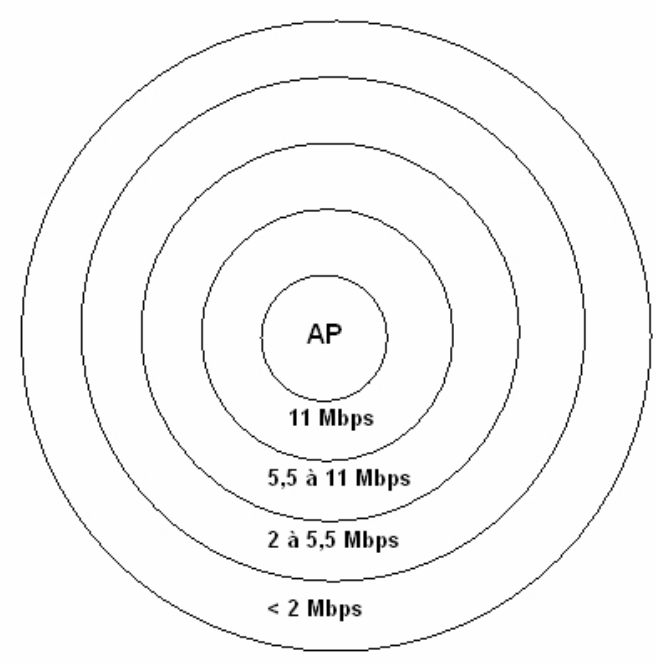
- Le multiplexage synchrone : les slots temporels sont pré assignés aux sources et fixés. Les slots assignés à une source sont transmis même si la source n'a rien à transmettre.
- Le multiplexage asynchrone : on ne transmet que si la source à quelque chose à transmettre.

2.7 Le wireless

Un réseau sans fil (en anglais wireless network) est, comme son nom l'indique, un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire. Les réseaux sans fil sont basés sur une liaison utilisant des ondes radioélectriques (radio et infrarouges) en lieu et place des câbles habituels. Les ondes sont véhiculées par l'air ; ces ondes sont donc absorbées par tous les obstacles qu'elles rencontrent. C'est pourquoi la portée et le débit sont plus faible qu'un réseau filière.
Il existe deux modes opératoires pour définir un réseau sans fil :

- Le mode infrastructure dans lequel les clients sans fils sont connectés à un point d'accès (access point). L'access point envoie régulièrement des ondes pour demander aux PC à portée s'ils veulent se connecter au réseau.
- Le mode ad hoc dans lequel les clients sont connectés les uns aux autres sans aucun point d'accès.

Le débit est partagé entre les utilisateurs et dépend de la portée, d'où on se situe :



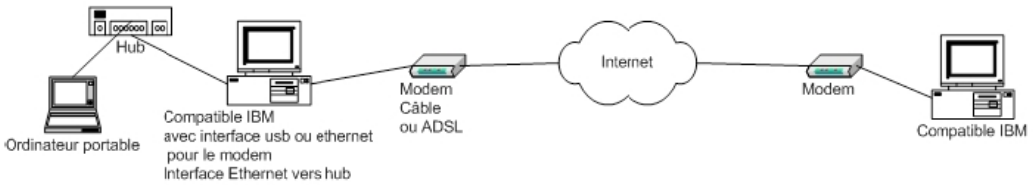
Chapitre 3

La couche liaison de données : Les connexions point à point, les réseaux

3.1 La couche Hote Réseau

Elle correspond aux deux niveaux inférieurs du modèle OSI.
Elle définit la couche Liaison de données et la couche physique.

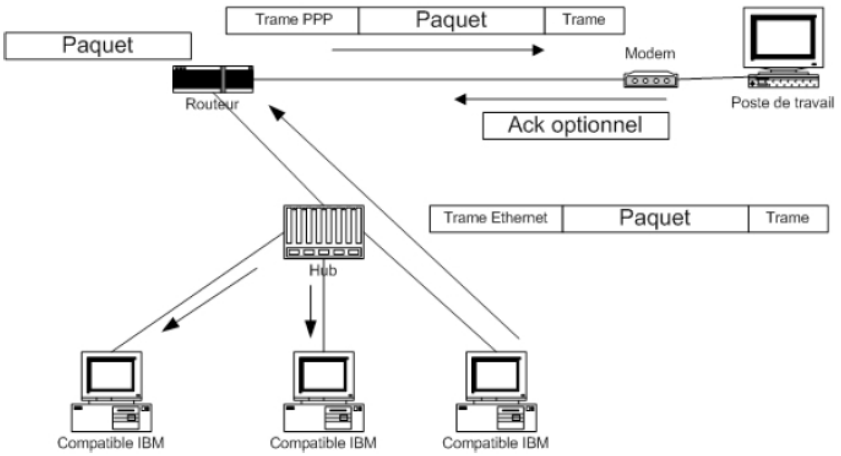
La couche physique (Physical Layer)



- Le modem + le câble de téléphone ou la carte réseau avec le câblage et le hub.
- Le niveau physique correspond aux règles et procédures à mettre en oeuvre pour acheminer les éléments binaires (0 ou 1) sur le médium physique. Autrement dit, cette couche est responsable de la conversion d'éléments binaires en signaux électriques qui seront transmis par un câblage ou des ondes radios.
- Les canaux sont répartis en deux catégories. Les canaux numériques et les canaux analogiques.
- Les canaux numériques sont surtout utilisés de préférence par les réseaux locaux
- Les canaux analogiques sont eux employés par les réseaux point à point.
- Représentation des 1 et 0 sur les lignes analogiques c'est le travail du modem.
  Un bon codage doit offrir une bonne résistance aux différentes interférences qui existent sur longue distance.
- Les lignes numériques disposent aussi d'un codage de l'information pour éviter que celle-ci soit trop sensible aux perturbations. On parle parfois à tort de modem numérique.
- Initialisation et relâchement de la connexion dans le cas des réseaux points à points.
- Problème de détecter les émissions simultanées sur un support partagé comme dans les réseaux locaux.

Les insuffisances de la couche physique
- Cette couche ne détecte pas et ne corrige pas les erreurs
- Elle n'offre aucun moyen de distinguer les données ou information d'adressage (ip, mac) dans un flux de bits .
- Aucune fonction d'adressage n'est offerte.
- Les hubs utilisés dans les réseaux ethernet recopient systématiquement l'information reçue sur tout les ports ce qui restreint la transmission ç une station. Le répeteur ne supporte pas non plus le full duplex (source : Spurgeon)

3.2 La couche Trame ou Liaison de données (Data Link Layer)



Définition. *La **trame** est l'entité transportée sur les lignes physiques. Elle contient un certain nombre d'octets transportés simultanément. Le rôle du niveau trame consiste à envoyer un ensemble d'éléments binaires sur une ligne physique de telle sorte qu'ils puissent être récupérés correctement par le récepteur.*

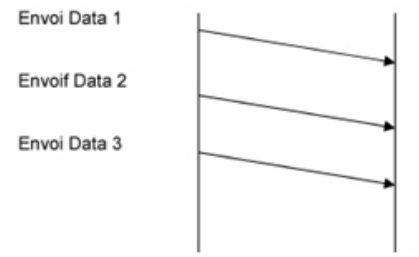
- C'est le protocole ppp ou la trame Ethernet
- La trame est une structure de données.
- Dans le cas des réseau locaux, le protocole le plus utilisé est Ethernet.
- ! Pour les réseaux points à point, le protocole le plus utilisé est ppp.
- Il est devenu courant pour les réseaux point à point d'utiliser des modems avec une connexion ethernet. Dans ce cas la trame ppp est encapsulée dans une trame ethernet.
- Les données sont découpées en trames (de l'ordre de 1000 octets).
- Ces trames seront transmises par la couche physique.
- Ces trames peuvent être acquittées par le récepteurs par des trames d'acquittement. On les appelle trame d'ack.
- Elle doit distinguer les trames dans le flux de bits fournis par la couche physique.
- Gérer les problèmes posés par les trames perdues, endommagées ou dupliquées.
- Empêcher qu'un ordinateur rapide inonde un ordinateur lent (contrôle de flux).
- Les switchs sont capables de lire les trames et d'extraire les adresses macs et optimiser le trafic en fonction de ces adresses.
- Certains switch peuvent partitionner le trafic réseaux
- Elle gère la communication directe entre deux machines/routeurs qui sont reliées directement par un canal de communication. Le protocole ppp (peer to peer protocol) est très utilisé pour connecter un pc à un routeur appartenant à un provider.
- Dans le cas des réseaux à diffusion, se pose le problème de l'accès au média qui est réglé par la sous-couche mac. Cette couche introduit les adresses physiques. Le réseau est partagé entre plusieurs machines et il faut bien remettre la trame à la bonne machine.

Remarques :
- PPP (peer to peer protocole) : distance élevée et faible débit ;
- Ethernet : débit élevé et faible distance.

3.3 Objectifs de la couche liaison de données

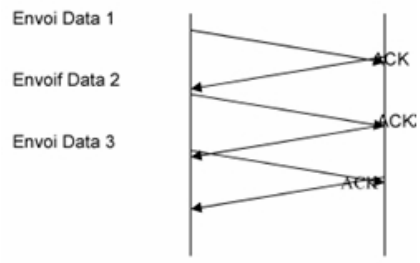
3.3.1 Les services offerts à la couche réseau

3.3.1.1 Le service sans connexion et sans accusé de réception



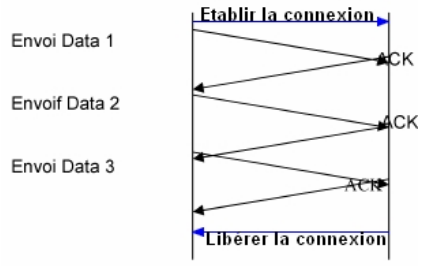
- Envoie des trames à la machine de destination sans recevoir d'accusés de réception de cette dernière.
- Pas de connexion établie au préalable.
- Utile quand le taux d'erreurs est faible et que la correction des problèmes est faite à un niveau supérieur.
- Usage : réseaux locaux, trafic temps réel (parole) où la vitesse est plus importante que la correction d'erreurs.
- C'est le mode de fonctionnement ethernet.

3.3.1.2 Le service sans connexion et avec accusé de réception



- Chaque trame émise est acquittée.
- Se justifie dans le cas de lignes physiques où le taux d'erreurs est élevé.
- Cette technique est utilisée par les réseaux sans fil.

3.3.1.3 Le service orienté connexion et avec accusé de réception



- Service le plus élaboré.
- Une connexion est établie au préalable.
- Chaque trame est numérotée et la couche liaison garantit que chaque trame envoyée est reçue une fois et une seule et dans l'ordre.
- Trois phases pour établir une connexion : établissement de la connexion, transmission des données, libération de la connexion.
- Le protocole PPP utilise cette technique.

3.3.2 La notion de trames

3.3.2.1 Remarques générales

– La couche physique véhicule un train de bits.
– La couche liaison découpe le train de bits en trames.
– On calcul une somme de contrôle qui est rajoutée à la fin de la trame.
– Le récepteur recalcule la somme de contrôle.
– Le découpage en trames et une opération délicate.

3.3.2.2 Les types de découpages en trames

1. Compter les caractères
2. Avoir des caractères de début de trame, de fin de trame et de transparence.
3. Utiliser des fanions (flags) de début et de fin de trame avec des bits de transparence.
4. Violer le codage de la couche physique.

3.3.3 Le contrôle d'erreur

- Utilisation d'un ACK (acquittement positif) ou NACK (acquittement négatif).
- En cas de perte de trame entière, l'émetteur attend en vain une trame d'acquittement → temporisateur (tinter) au niveau de l'émetteur qui retransmettra la trame.
- Si la trame et l'acquittement sont perdus, le temporisateur se déclenchera plusieurs fois → le récepteur recevra plusieurs fois la même trame. Il est donc important de numéroter les trames pour les distinguer et évier ainsi de délivrer plusieurs fois la même trame.

3.3.4 Le contrôle de flux

- Le problème se pose quand un ordinateur émetteur transmet plus de trames que le récepteur ne peut en accepter ? perte inévitable de trames.
- La solution consiste à instaurer un contrôle de flux pour contraindre l'émetteur de ne pas envoyer plus de trames que le récepteur ne peut en recevoir.
- Le principe de base : impossible d'envoyer des trames sans avoir au préalable une permission implicite du récepteur.

3.4 Détection et correction des erreurs

3.4.1 Les codes correcteurs d'erreurs

Nombre de bits nécessaires : L'idée est la suivante : rajouter des bits de contrôles aux bits de données avec comme objectif de détecter les bits erronés. L'équation suivante donne le nombre de bit de contrôle r à rajouter à m bits transmis pour trouver les erreurs simples :

$$(m + r + 1) <= 2^r$$

Effectuons le calcul suivant avec $m = 7$:

$$\begin{aligned}(7 + 0 + 1) &<= 2^0\\ (7 + 1 + 1) &<= 2^1\\ (7 + 2 + 1) &<= 2^2\\ (7 + 3 + 1) &<= 2^3\\ (7 + 4 + 1) &<= 2^4\end{aligned}$$

Ce qui nous donne $r = 4$ soit 4 bits de contrôles. On doit donc rajouter plus de 50% du nombre de bits transmis. Cela limite donc l'usage qu'on en fait.

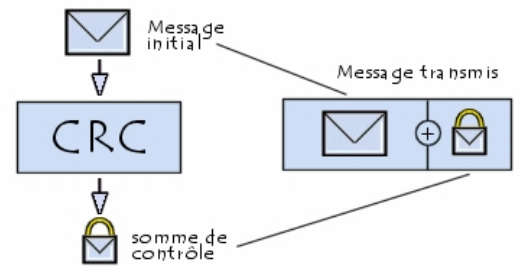
3.4.2 Les codes détecteurs d'erreurs

Objectif : Détecter les erreurs qui se seraient produites lors du transfert d'une trame sur le réseau.

La théorie : Le principe du CRC consiste à traiter les séquences binaires comme des polynômes binaires. Dans ce mécanisme de détection d'erreur, un polynôme prédéfini (appelé polynôme générateur) est connu de l'émetteur et du récepteur. La détection d'erreur consiste pour l'émetteur à effectuer un algorithme sur les bits de la trame afin de générer un CRC, et de transmettre ces deux éléments au récepteur. Il suffit alors au récepteur d'effectuer le même calcul afin de vérifier que le CRC est valide.

La trame aura donc une allure comme suit :

En-tête	destination @ sources	Données	Valeur CRC



3.5 La couche liaison dans les lignes point à point

3.5.1 Les types de lignes point à point

Définition. *Une **ligne louée** fournit un circuit dédié toujours actif entre deux points d'extrémité. Le fournisseur de services achemine simplement un flux de bits à un débit constant ; il n'effectue aucune interpretation ni ne prend aucune décision sur les bits transmis.*
Cette option est la plus couteuse pour une entreprise.

Définition. *Une **commutation de circuit** fournit une bande passante dédié entre deux points, mais seulement pendant la durée de l'appel. Sert habituellement d'alternative plus économique aux lignes louées, surtout quand une connectivité permanente n'est pas requise. Représente aussi une solution de secours utile en cas de défaillance d'une ligne louée ou d'un service de commutation de paquets.*
Option d'un cout raisonnable si on echange pas systématiquement des informations

Définition. *Une **commutation de paquets** fournit des circuits virtuels entre des sites prix deux à deux, avec des débits définis contractuellement pour chaque circuit . La connectivité physique au niveau de chaque site consiste en une ligne louée raccordée à un équipement sur le réseau du fournisseur de services.*
Cette option revient généralement moins cher que les lignes louées.

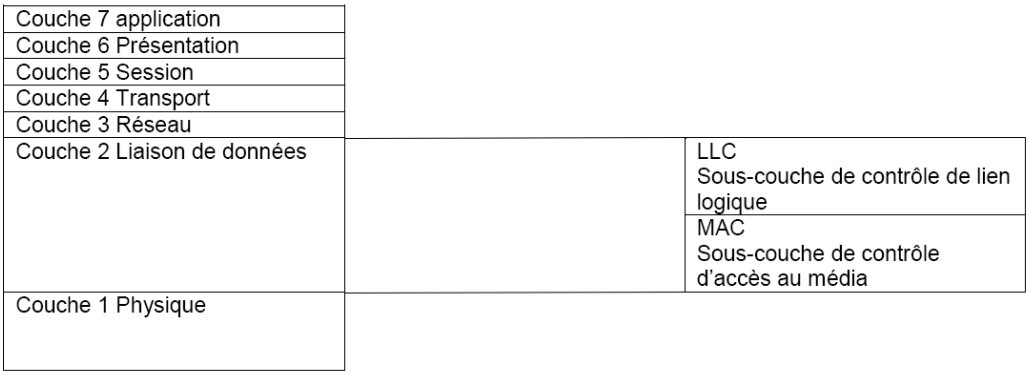
3.5.2 Le protocole PPP

Définition. *Le protocole **Point to Point Protocol (PPP)** est un protocole de type liaison de donnée point à point qui permet le transport d'IP sur des lignes analogiques ou numériques.*

Ce protocole procure bien plus qu'une simple connexion entre hôtes. Il définit aussi différentes fonctions de gestion et de test qui tiennent compte de a qualité de la ligne, les options de négociations et l'attribution d'adresses IP.

3.6 La couche liaison et les réseaux de type diffusions MAC : La sous couche de contrôle d'accès au canal

3.6.1 Introduction



La couche liaison que nous venons de voir est principalement dédiée aux réseaux point à point. Dans ce type réseau, il n'a pas de problème de partage du canal de transmission puisqu'il n'y a qu'un émetteur. Les réseaux de Type WAN sont très souvent du type point à point.
Dans les réseaux locaux, il peut y avoir plusieurs émetteurs. Il se pose alors le problème de savoir qui sera le prochain émetteur : l'élu.
Les protocoles utilisés pour déterminer qui sera le prochain élu d'un canal de communication à accès multiple sont regroupés dans une sous couche interne à la couche liaison de données appelée sous- couche de contrôle d'accès au canal ou sous-couche MAC.

3.6.2 La sous couche MAC sous Ethernet

3.6.2.1 CSMA/CD ou CSMA avec détection des collisions

Ce terme signifie **Carrier Sense Multipe Access with Collision Detection**.
Cette technique est le standard sous Ethernet. A l'écoute préalable du réseau, comme toutes les méthodes CSMA s'ajoute l'écoute pendant la transmission d'où l'ajout du terme *cd* : un coupleur prêt à émettre, ayant détecté un canal libre, transmet et continue à écouter le canal. De ce fait, il se produit une **collision**, il interrompt dès que possible sa transmission et envoie des signaux spéciaux, appelés **bits de bourrage**, afin que tous les adaptateurs soient prévenus de la collision. Il tentera de nouveau son émission ultérieurement après un certain laps de temps qui est calculé par l'**algorithme de backoff**.

3.6.2.2 L'algorithme de backoff

Après chaque collision, la carte ethernet va attendre ce que l'on appelle un certain nombre de **slots times**.

Définition. *Un **slot time** est le temps de propagation maximum du signal dan un réseau aller et retour. Il vaut 512 bit times (temps de propagation d'un bit) ou 51,2 micro-secondes.*

Le principe de l'algorithme consiste après un échec de transmission à attendre un laps de temps aléatoire. Si les collisions se répètent à nouveau, on attend de plus en plus longtemps. L'objectif de l'algorithme est de faire en sorte que les adaptateurs ne demandent pas tous en même temps le support de transmission en répartissant leurs demandes dans le temps.

Algorithme :

1. Ecouter le média
   - Si occupé → attendre puis recommencer à 1
   - Si libre → on va au 2
2. Envoie des données avec écoute du média pour regarder
   - Si colision → envoie des bits de bourrage, attendre, puis recommencer à 1
   - Si OK → terminer

Nombre de collisions préalables	Temps d'attente maximum
1	0 ou 1 slot time
2	0 ou 1 ou 2 ou 3 slots times
3	2^3 slots times
16	2^{16} slots times Après 16 tentatives, on arrête

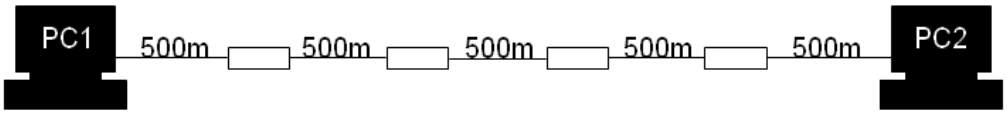
Le format de la trame DIX : Standard originel proposé par Digital Intel Xerox. Il est le plus utilisé.

64bits	48bits	48bits	16bits	46 à 1500 octets	32bits
Préambule	Destination	Source	Type	Données	CRC

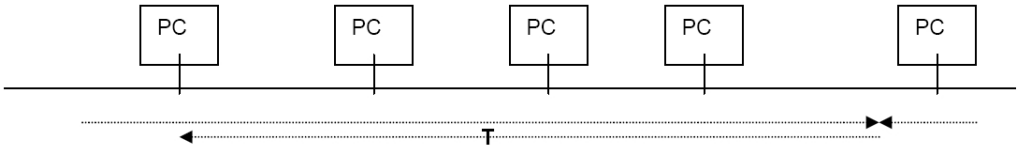
Nom du champ	Description
Préambule	64 bits qui sont destiné à permettre à l'électronique de la carte de s'appercevoir qu'une transmission est en cours
Adresse de destination	Le premier bit indique le type d'adresse 1 : Adresse Multicast 0 : Adresse Physique Appelée souvent Adresse mac ou encore Adresse Physique
Adresse source	Idem à l'exception du premier bit
Type	Donne le type de protocole de niveau supérieur. Par exemple, TCP/IP
Données	46 à 1500 octets. La partie donnée fait toujours 46 octets minimums
CRC	Le CRC est un nombre unique généré en appliquant un calcul de polynôme au modèle de bits qui constituent la trame

La trame fait au minimum 512 bits (on ne tient pas compte du préambule parce qu'il ne contient pas des choses intéressantes).
Donc si on a un réseau de 10 Mbps, la trame sera envoyée en 51,2 micro seconde (ce qui correspond au slot time). On en déduit donc que les collisions doivent être plus rapide c'est à dire inférieure à 51,2 micro secondes.

Un réseau Ethernet peut faire maximum 2500m à cause des collisions. En effet, il faut que les bits de bourrages envoyés par le PC1 puissent atteindre le PC2.



Le problème de la détection des collisions



- Il faut émettre pendant $2T$ au moins pour être certain de détecter toutes les collisions, avec T le temps de propagation jusqu'aux extrémités. Si un signal est émis, il doit se progager jusqu'aux extrémités et si une collision se produit, il faut lui laisser le temps de revenir.
- Dans un réseau de 10 Mbps et pour une distance de 2500/2800 mètres incluant quatre répéteurs, le temps $2T$ est égal à 51,2 micro-secondes.
- Ce temps correspond à l'émission de trames de 64 octets.

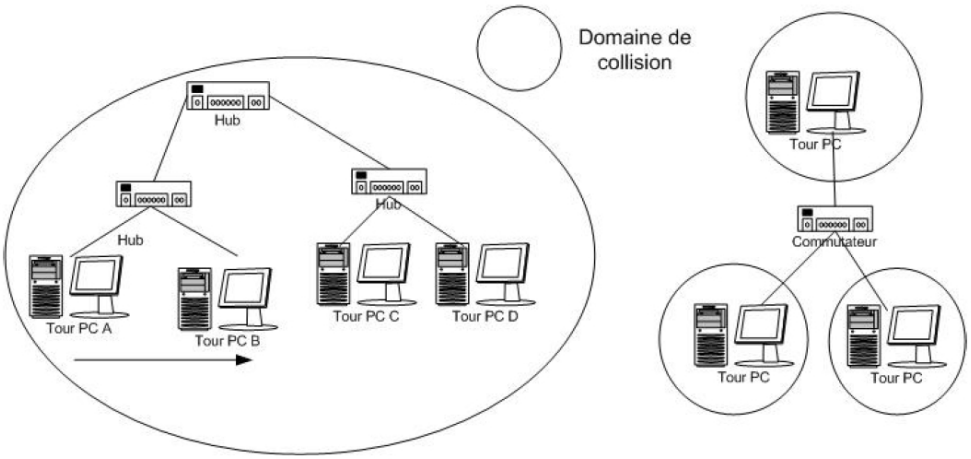
Dans un réseau de 100 Mbps et pour une distance de 220/250 mètres incluant quatre répéteurs, le temps $2T$ est égal à 5,12 micro-secondes.

Dans un réseau de 1 Gbps et pour une distance de 20 mètres incluant quatre répéteurs, le temps $2T$ est égal à 0,512 micro-secondes.

Comportement en cas de collisions

- Arrêt immédiat de la transmission
- Emission d'un signal de brouillage pour renforcer la collision.
- Attente aléatoire, entre 0 et 1023 slots.
- Un slot vaut 51,2 micro-secondes (soit la transmission de 512 bits)

Définition. *Un **domaine de collision** est formellement défini comme un seul réseau CSMA/CD dans lequel il se produira des collisions si deux stations attachées au système transmettent au même moment. Il ne faut pas dépasser 20 à 30 machines.*



3.7 La norme IEEE 802.3 et réseau Ethernet

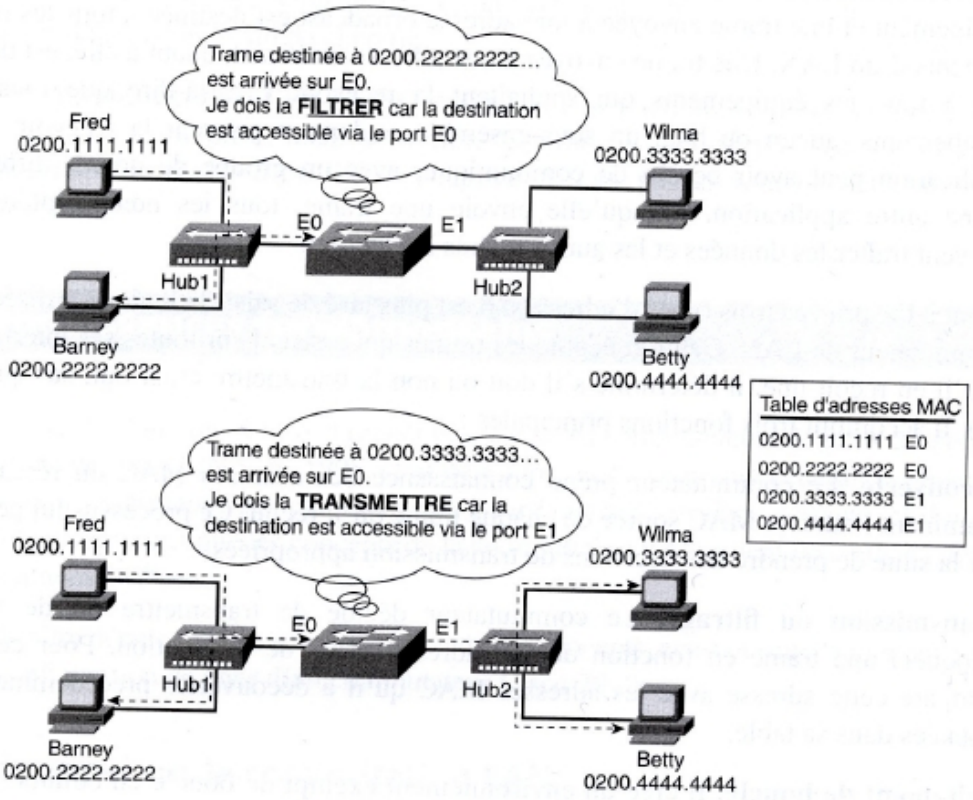
3.7.1 Les réseaux commutés

3.7.1.1 introduction

Les ponts et les commutateurs servent à relier des segments ethernet.
Ils s'affranchissent des limites imposées par les domaines de collision.
Ils peuvent relier des segments à des vitesses différentes.
Les segments sont reliés à des ponts via des ports.
Autrefois on utilisait le terme pont (bridge). De nos jours , le terme commutateur(switch)est préférable pour désigner ces équipements.

3.7.1.2 Décision de transmission ou filtrage

Les interfaces des ponts fonctionnent en **mode promiscuité** et lisent toutes les trames qui passent sur le segment. Chaque trame contient deux adresses : la source et la destination.
Les commutateurs limitent la surcharge du réseau en ne transmettant d'un segment à un autre que le trafic qui en vaut la peine. Pour distinguer les trames à acheminer de celles qui doivent être filtrées, ils s'appuient sur une table appelée **table de pontage** ou **table d'adresses MAC** qu'ils construisent dynamiquement. Chaque fois qu'un commutateur reçoit une trame, il consulte sa table pour prendre une décision adéquate.



Le commutateur décide de filtrer la trame que fred envoie à Barney. Celle-ci porte l'adresse MAC 0200.2222.2222 qui correspond à celle de Barney. Le commutateur reçoit cette trame car il est relié au hub1. Filtrer signifie que la trame n'est pas retransmise vers les autres ports du switch.
Par contre la trame que Fred transmet à Wilma est transmise uniquement sur le port E1 car en consultant sa table, le commutateur a noté que L'adresse destination de Wilma (0200.3333.3333) est associée au port E1.

3.7.1.3 La découverte d'adresses

Au lieu d'entrer manuellement les adresse de destination dans le commutateur, on a choisit une approche dynamique.
Au départ la table de commutation est vide. Le commutateur construit sa table en écoutant les trames entrantes et en examinant leur adresse MAC source. Si l'adresse MAC source ne se trouve pas dans la table, une entrée est crée dans la table . Cette entrée est constituée d'une association Mac interface.
Les associations (adresse MAC & port) sont **limitées dans le temps**.
Dans le schéma ci-dessus, Fred a envoyé une première trame à Barney. Le commutateur ajoute une entrée pour l'adresse mac de Fred 0200.1111.1111, en l'associant à l'interface E0. Quand Barney répond, le commutateur ajoute une seconde entrée pour l'adressse MAC de ce dernier 0200.2222.2222 avec la valeur E0. Le traffic ne doit pas traverser le switch pour être incorporé dans la table de commutation et c'est toujours l'adresse source qui est prise en considération.

3.7.1.4 Acheminement du traffic unicast à destination inconnue et du trafffic broadcast

Comme le traffic broadcast doit être reçut par toutes les machines d'un LAN, un commutateur relaie toujours sur tous ses ports le traffic broadcast a l'exception du port de réception.
Le traffic unicast inconnu (non présent dans la table cam) est aussi propagé de la même manière dans l'espoir que le destinataire inconnu se trouve sur un des segments ethernet et réponde ce qui créera une entrée dans la table.
Même technique pour le traffic multicast.

3.7.1.5 Synthèse logique de transmission d'un commutateur

1. Une trame est reçue.
2. Si l'adresse de destination est broadcast ou multicast, la trame est transmise sur tous les ports à l'exception de celui de réception.
3. Si l'adresse de destination est unicast et qu'elle est absente de la table, la trame est transmisse sur tous les ports à l'exception de celui de réception.
4. Si l'adresse de destination est unicast et qu'elle est présente dans la table , et si l'interface associée n'est pas celle de réception, la trame est transmise sur le port approprié.
5. Sinon la trame est filtrée (bloquée)

3.7.2 Les modes de retransmission interne des trames

La trame doit toujours être analysée par le commutateur.
Il existe trois techniques d'implémentation des trames.

1. La méthode Store and Forward
2. La méthode Cut and Through
3. La méthode Fragment - Free

3.7.2.1 La méthode Store and Forward

Cette approche utilisée par la plupart des commutateurs consiste à mémoriser la trame totalement. Si la trame est incomplète ou présente un mauvais CRC, elle n'est pas retransmise. Ceci évite un encombrement inutile du réseau.
Toutefois, le stockage introduit un délai de traitement. Le délai de transmission des informations dépend aussi de la taille des trames.

3.7.2.2 La méthode Cut and Through

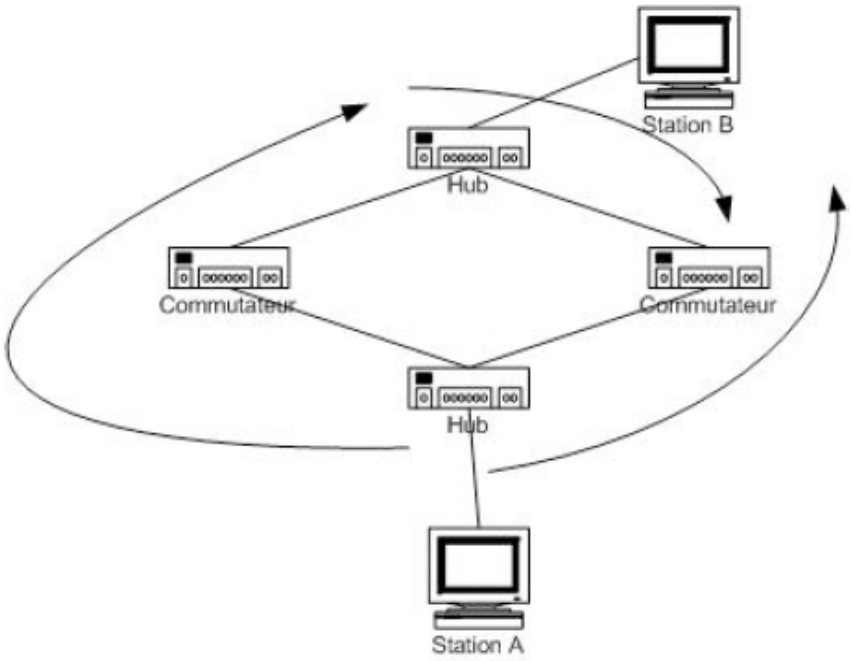
Cette méthode consiste à stocker uniquement le début de la trame et dès que l'adresse du destinataire est identifiée, la trame est transmise vers le port de destination, avant même la fin de réception de la trame.
Le délai de traitement est diminué mais des trames endommagées encombrent inutilement le réseau.

3.7.2.3 La méthode Fragment - Free

Cettte méthode est une évolution de la Cut and Through. Ici on attend de lire les 64 premiers octets avant de retransmettre la trame sur le port concerné car si il y a collision elle est normalement détectée quand les 64 premier octets sont émis. Ici le commutateur ne transmettra pas les trames endommagées sur le réseau et le temps de latence reste bas.

3.7.3 L'algorithme du spanning tree (arbre en expansion) ou STP

3.7.3.1 Le problème des boucles



Le mécanisme que nous venons de décrire rencontre des problèmes quand deux commutateurs sont reliés en boucle :

1. Broadcast storm : le switch recopier les trames broadcast sur tous les ports
2. Copies multiples de trames inutiles
3. Instabilité des tables de commutation

Exemple :
Une trame émise par la station A (port 1) vers la station B (port 2) est lue par deux ponts.
Ces ponts interconnectent les segments A et B.
Les deux ponts lisent la trame coté 1 et marquent l'origine comme étant Port 1 pour A.
La station B reçoit deux trames identiques.
Les deux trames sont reçues par les deux ponts coté 2 (chacun lit la trame de l'autre).
Les deux trames sont réexpédiés sur le coté 1 et marquent l'origine comme étant Port 2 pour A.
La station A devient inaccessible un bref instant puisqu'elle est coté A.

3.7.3.2 Présentation du Spanning Tree Protocol

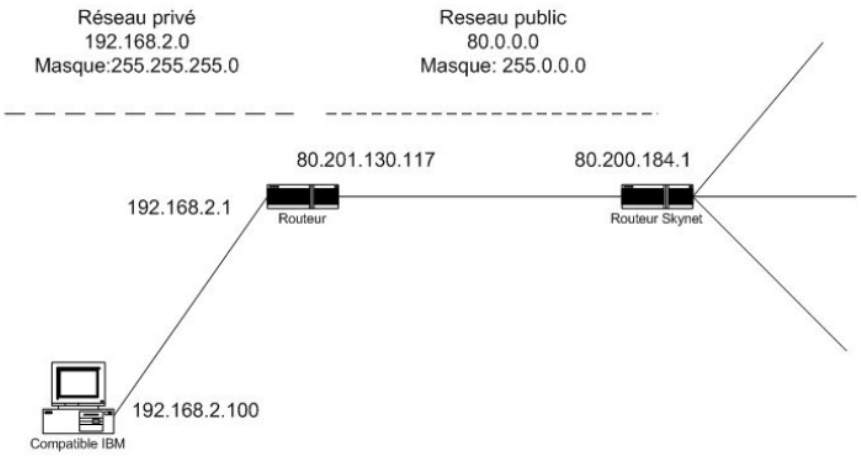
Le protocole STP place chaque port de pont/Commutateur dans un état de Transmission (Forwarding) ou de blocage (blocking).
Les ports qui se trouvent dans un état de transmission forment ce que l'on appelle un arbre recouvrant (spanning tree) ou arbre STP. Cet arbre définit un chemin unique pour transmettre les trames entre les segments Ethernet. Les ports dans l'état forwarding peuvent envoyer et recevoir des trames. Ce n'est pas le cas de ceux qui se trouvent dans un état de blocage.

Chapitre 4

La couche réseau, le routage

4.1 Introduction

4.1.1 La couche réseau (Network Layer) : ses fonctions



- Cette couche gère des paquets. Ces paquets sont transportés par des trames de la couche 2. Les trames les plus courantes sont ethernet et ppp.
- Quand la trame arrive au routeur, la couche liaison de ce dernier extrait le paquet et c'est à charge de la couche réseau du routeur de déterminer la ligne de sortie en se basant sur la topologie du réseau.
- Elle se sert pour cela des adresses logiques qui sont contenues dans les paquets. Il existe deux adresse : la source et la destination. L'adresse logique sert à identifier de manière unique chaque interface réseau. Comme une machine peut avoir plusieurs interfaces, une machine peut avoir plusieurs ip.
- L'adressage est structuré mais cette structure garantit l'unicité. L'adresse IP est lui structuré à deux niveaux : le réseau logique et le numéro d'hôte (c'est le masque qui donne le numéro de réseau).
- La couche réseau permet de découper un réseau physique en plusieurs réseaux logiques. Sur le schéma ci-dessus, deux réseaux logiques sont illustrés.
- Chaque réseau logique se voit attribuer un numéro qui est unique et toutes les machines appartenant au même réseau logique auront le même numéro de réseau si on applique le masque.
- Chaque machine possède une table de routage. C'est l'adresse de destination qui va déterminer la ligne de sortie via la consultation de la table. On appelle cela en terminologie réseau le routage. C'est la fonction principale de la couche réseau
- Plutôt que d'avoir une entrée pour chaque hôte, on place une entrée pour chaque réseau logique sachant que chaque hôte appartient toujours à un réseau.
- Le routage peut être basé sur des tables statiques contenues dans les routeurs. Une table statique est obtenue par encodage manuel de l'opérateur.
- Le routage peut être basé sur des tables dynamiques contenues dans les routeurs. Ces tables sont obtenues par échange dynamique d'informations avec d'autres routeurs.
- La couche réseau gère la notion la notion de réseau privé et public.

– Un réseau privé est interne à une entreprise et n'est pas visible en principe depuis l'extérieur.
– Un réseau public est accessible à tout le monde et pour garantir cet accès, chaque machine doit recevoir une adresse publique qui sera attribuée en fonction de la localisation de la machine par un organisme agréé.
– Un ordinateur qui appartient à la fois à un privé et qui souhaite accéder à un réseau public devrait avoir une adresse privée et publique.
– Un routeur d'entreprise dispose au moins d'une interface publique et privée. Il dispose au moins d'une adresse privée et d'une adresse publique.
– La technologie nat permet à un routeur de partager son adresse publique entre des machines privées qui souhaitent accéder comme client internet. Tous les paquets sortiront avec l'adresse de l'interface publique du routeur.

4.1.2 Structure d'un paquet

<table>
<tr><td colspan="5">32 bits</td></tr>
<tr><td>Version</td><td>Longueur entête</td><td>Type de service</td><td colspan="2">Longueur totale</td></tr>
<tr><td colspan="3">Identification</td><td>Drap</td><td>Dep_fragment</td></tr>
<tr><td colspan="2">Protocole</td><td colspan="3">Total de contrôle d'en-tête</td></tr>
<tr><td colspan="5">Adresse source</td></tr>
<tr><td colspan="5">Adresse de destination</td></tr>
<tr><td colspan="5">Options</td></tr>
<tr><td colspan="5">Données</td></tr>
</table>

4.2 Généralités sur la couche réseau

4.2.1 Evolution de la couche réseau

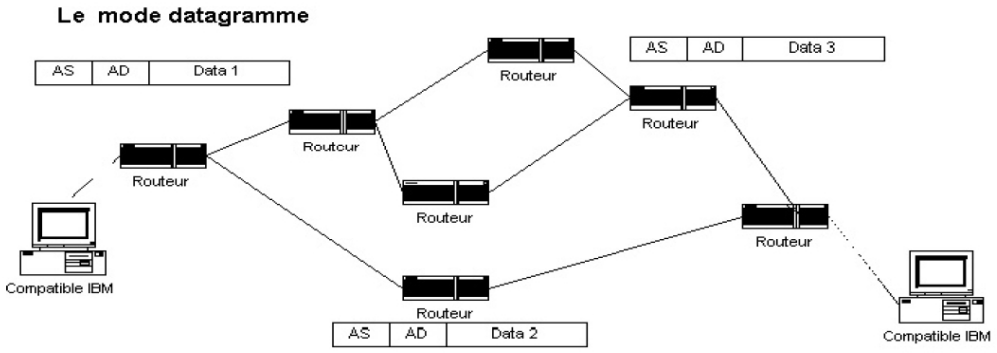
4.2.1.1 La ligne louée

On appelle **lignes "louées"** des lignes spécialisées qui permettent la transmission de données à moyens et hauts débits (64 Kbps à 140 Mbps) en liaison point à point : l'opérateur de télecom place une ligne spécifique à la demande du client entre les points qu'il souhaite relier. L'exemple typique est la connexion d'une agence bancaire à son site central.

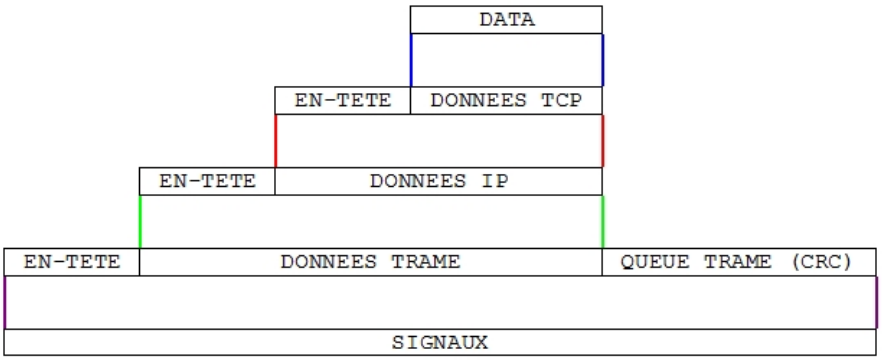
4.2.1.2 Commutation de circuits

Le réseau téléphonique (non Gsm) est constitué des téléphones des abonnées et d'une série de commutateurs. Les commutateurs forment une hiérarchie. Il y'a des commutateur au niveau zonal et régional.
L'abonné ou l'entreprise est raccordé à un commutateur via une ligne qu'il loue à l'opérateur de télecom.
Quand une personne établit une communication avec une autre, un circuit physique est établi à l'intérieur des commutateurs le temps de la durée de la communication téléphonique.
Le circuit est réservé pour la durée de la communication. Ceci explique la tarification à la durée, sachant que l'abonné à un usage exclusif du circuit.

4.2.1.3 Commutation de paquets



- Les lignes disposent de tampons en entrée et en sortie.
- Ces tampons peuvent contenir des paquets qui sont générés par les ordinateurs.
- Les paquets ont une taille fixe et c'est à charge des machines de découper l'information à l'envoi et la reconstituer à la réception.
- Le passage de l'information se fait en recopiant le paquet du tampon d'une ligne vers le tampon d'une autre ligne. Quand la ligne transmet le paquet elle l'encapsule de nouveau dans une trame (schéma ci-dessous).
- Chaque paquet contient une adresse source et destination.
- L'adresse destination (adresse logique) sert au routeur à déterminer la ligne de sortie pour chaque paquet entrant.
- La décision est effectuée sur la base d'une table de routage qui indique pour chaque adresse la ligne de sortie à utiliser. Si le routeur ne trouve pas l'adresse, une entrée par défaut indique la ligne de sortie à utiliser.
- La transmission de paquets ne requiert pas la réservation d'une connexion. La ligne est toujours disponible pour l'ensemble des usagés. La limite vient ici du nombre de paquets qu'une ligne peut transmettre par seconde. Quand les lignes sont saturées on parle de congestion.
- On peut comparer le réseau à commutation de paquets à un réseau routier.
- Si un routeur tombe en panne, les autres routeurs peuvent le détectent et choisir un autre chemin pour les paquets suivants.



4.3 La couche réseau dans internet

4.3.1 Internet, qu'est-ce que c'est ?

Définition. ***Internet*** *est un réseau global constitué de réseaux distincts permettant aux ordinateurs de toute sorte de communiquer et partager des services directement et de manière transparente.*

4.3.2 Les adresses IP

4.3.2.1 Les fonctions de l'adresse IP

La première fonction est d'identifier de manière unique un hote sur internet.
La seconde fonction de l'adressage IP est de cloisonner le réseau physique en réseaux logiques afin de cloisonner le trafic réseau. On vise à créer l'équivalent des partitions logiques des disques durs. L'adresse IP est décomposée en l'identifiant réseau et l'identifiant ordinateur. Les machines. appartenant à un même réseau logique auront le même identifiant réseau.

4.3.2.2 Le rôle du routeur

C'est le routeur qui donne vie aux réseaux logiques. Un routeur gère un réseau logique par interface ou autrement dit chaque interface donne accès à un réseau logique.

4.3.2.3 Le routeur vs hub vs switch

Domaine de collision : zone ou il y a collision quan il y a émission simultanée.
Domaine de broadcast : liste des interfaces recevant un broadcast.

Périphérique	Domaine
HUB	1 domaine de collision 1 domaine de broadcast Ne gère pas les réseaux logiques
SWITCH	1 domaine de collision par interface 1 domaine de broadcast Ne gère pas les réseaux logiques
ROUTEUR	1 domaine de collision par interface 1 domaine de broadcast par interface 1 réseau logique par interface

4.3.2.4 La structuration de l'adresse ip

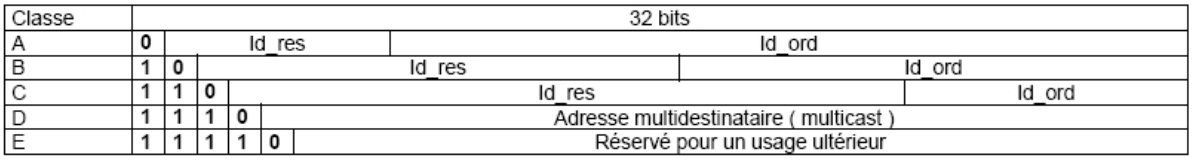
Une adresse réseau IP se représente sous forme de 4 octets en représentation décimale séparés par un point. L'adresse ip est décomposée en deux parties :
L'identifiant réseau (netid) et l'identifiant du hôte (hostid)

32 bits	
Netid	Hostid
N bits	32 - N bits

Un **masque** lui est toujours associé. Il détermine la partie réseau de l'adresse c'est à dire le Netid. Un & logique entre un masque réseau et une adresse réseau donne toujours le Netid.
Seules deux machines possédant le même netid peuvent communiquer ensemble directement. Des machines avec un netid différent doivent passer par un routeur ou nécessiter une configuration de leurs tables de routage.

4.3.2.5 Les classes d'adresses

Internet a définit 5 classes d'adresses. Ces classes fixent le masque d'office. Les trois premières sont réellement utilisables sous internet. Les premiers bits déterminent la taille de la partie de l'identifiant réseau.



4.3.2.6 Les capacités des adresses

Classe	Nombre de réseaux	Nombre de machines
A	$2^7 - 2$ (7bits)	16 millions (2^{24})
B	16382 (14bits)	65 536 (2^{16})
C	2millions (21bits)	254

Classe	Bytes Réseau	Nombre de réseaux	Bytes Hote	Nombre de Hotes
A	1 (7bits)	$2^7 - 2$	3 (24 bits)	$2^2 - 2$
B	2 (14bits)	$2^{14} - 2$	2 (16 bits)	$2^{16} - 2$
C	3 (21bits)	$2^{21} - 2$	1 (8 bits)	$2^8 - 2$

4.3.2.7 L'étendue des adresses IP

Classe	Class bits	Masque	Premier Net id utilisable	Dernier Net id utilisable	Comment
A	0	255.0.0.0	1.0.0.0	126.0.0.0	
B	10	255.255.0.0	18.1.0.0	191.254.0.0	
C	110	255.255.255.0	192.0.1.0	223.255.254.0	
D	1110	-	224.0.0.0	239.255.255.254	Non disponible pour un usage général
E	1111	-	240.0.0.0	255.255.255.254	Non disponible pour un usage général

Les numéros de réseau réservés : 127.0.0.0 , 128.0.0.0 , 191.255.0.0 , 192.0.0.0 et 223.255.255.0

4.3.2.8 Comment attribuer des ip à des pc

Dans l'exemple, on suppose que les pcs sont branchès à un hub ou à un switch.
(1) 111.112.113.114
(2) 111.112.113.115
(3) 111.112.115.114
(4) 111.112.115.115
Masque : 255.255.255.0
(1) peut communiquer avec (2) , (3) avec (4) mais pas (3) avec (1) et (2) car ils n'ont pas le même netid qui est 111.112.113.0 pour les deux premiers et 111.112.115.0 pour les deux derniers.

(1) 111.112.113.114
(2) 111.112.113.115
(3) 111.112.115.114
(4) 111.112.115.115
Masque : 255.255.0.0
Tous peuvent communiquer car ils ont le même netid.

Définition. *Si deux **interfaces réseaux de niveau ip** doivent **communiquer** ensemble, il faut qu'ils aient une adresse réseau avec le même netid. Dans cas contraire il faudra intercaler un routeur entre les deux.*

4.3.2.9 Les adresses réservées

- Les numéros réseaux 127.X..X.X ou X.X.X est n'importe quel jeu de numéros. Ceci est utilisé pour une boucle locale de test software.
- Un numéro constitué uniquement de 0 est sans classe et signifie « mon réseau courant dont je ne connais pas le numéro courant ».
- Une partie hôte avec comme numéro 0 est réservée pour désigner un réseau particulier. Par exemple, 192.1.0.1 est la première adresse de classe C qui peut être allouée.
- Une partie hôte avec tout des 1 est réservée pour envoyer un broadcast à tous les hôtes sur un réseau spécifique. Il peut être utilisé seulement comme adresse de destination.
- L'adresse 0.0.0.0 est réservée. Elle est utilisée de deux manières : comme une adresse source quand le hôte ne connaît pas son adresse propre, et par les routeurs dans une liste d'adresses pour indiquer la route par défaut, la route pour tous les réseaux qui ne sont pas mentionnés.
- L'adresse pleine 255.255.255.255 est réservée pour une adresse de destination qui signifie cast vers tous les hôtes sur mon réseau. 0.0.0.0 est une forme obsolète de 255.255.255.255.

4.3.3 Les adresses de réseau publique/privé

4.3.3.1 Les adresses publiques

Chaque fois que l'on se connecte à Internet, une adresse publique est nécessaire.
Une adresse publique est une adresse qui est délivrée par L'IANA (Internet Assigned Numbers Authority) ou ses intermédiaire. Cette adresse va nous identifier de manière unique sur internet.

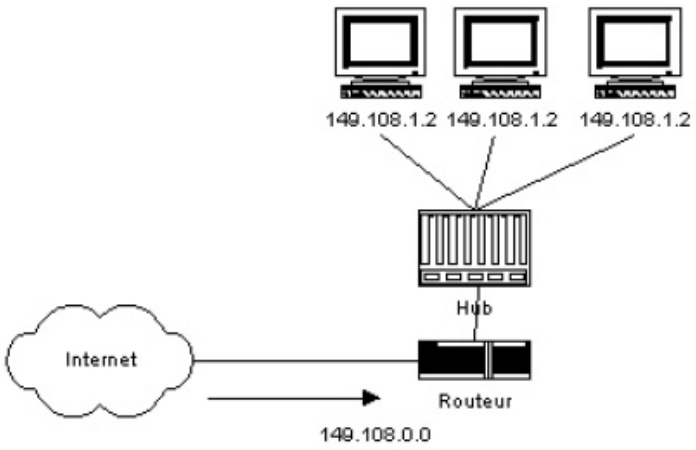
4.3.3.2 Les adresses privées

Définition. *Une **adresse privée** est une adresse ip qui n'a pas été attribuée par l'IANA et qui est utilisée dans un réseau interne.*

Définition. *Un **réseau privé** est un réseau ou les machines ou équipements ont des adresses qui ne sont pas attribuées officiellementparl'IANAetquiparconséquentnesontpasaccessiblesdirectement.*

4.3.4 Les sous-réseaux

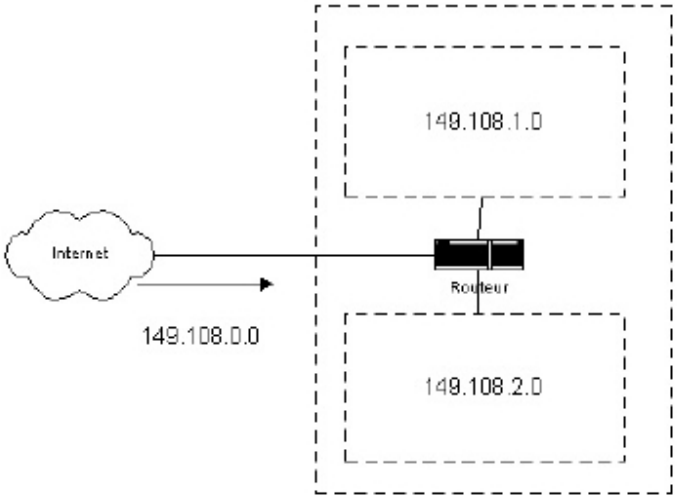
4.3.4.1 La problématique



Tous les ordinateurs appartenant à un même réseau doivent posséder le même identifiant de réseau.
- Une entreprise commence avec une adresse de classe B.
- Pour des raisons de sécurité et de rendement, il faut au moins deux réseaux distincts (Par exemple Marketing et Personnel).

– Il faut alors demander une nouvelle adresse au NIC.
– Le NIC doit alors informer la communauté Internet et les bases de données doivent être mises à jour dont le fameux DNS.
– Problème quand un ordinateur change de réseau vers un autre, cela nécessite une nouvelle adresse IP et la mise à jour L'ordinateur qui prendra l'ancienne adresse IP recevra le courrier électronique jusqu'à ce que la communauté Internet soit au courant.

4.3.4.2 La solution



– Une solution : partitionner le réseau d'entreprise en plusieurs entités à usage interne, alors que l'ensemble apparaîtra comme un seul à l'extérieur.
– Ces entités sont appelées des sous-réseaux

4.3.4.3 La démarche de créer des sous-réseaux

Définition de sous-réseaux

1. Déterminer le nombre d'ID de réseaux nécessaires pour l'utilisation courante en fonction des besoins de croissances prévus.
2. Déterminer le nombre maximum d'adresses d'hôtes sur chaque sous-réseau, toujours en anticipant des besoins de croissance prévus.
3. Définir un masque de sous-réseau pour tout l'interréseau, qui donne le nombre voulu de sous- réseaux et assez d'hôtes par sous-réseau.
4. Déterminer les ID de réseaux résultants à utiliser.
5. Déterminer les ID d'hôtes valides et attribuer des adresses Ip aux hôtes.

Déterminer le nombre d'ID de réseaux nécessaires

– Définir le nombre de sous-réseaux nécessaires en anticipant les besoins futurs.
– Un seul Id réseau est nécessaire pour chaque sous-réseau et connexion WAN.

Déterminer le nombre d'ID d'hôtes par réseau

Un ID hôte est nécessaire pour
- Chaque carte d'interface de réseau d'ordinateur TCP/IP.
- Chaque carte d'interface de réseau d'imprimante TCP/IP.
- Chaque interface de routeur sur chaque sous-réseau. Par exemple, si un routeur est connecté à deux sous-réseaux, il doit avoir deux ID d'hôtes, donc deux adresses IP.

Le même masque de sous-réseau doit être utilisé partout. Le nombre maximum de sous-réseaux et d'hôtes par sous-réseau est donc prédéterminé par le masque de sous-réseau choisi. Il faut penser à anticiper le futur.

Définir le masque de sous-réseau
Déterminez le nombre de sous-réseaux dont vous avez besoin. Attention créer des sous-réseaux, va diminuer le nombre d'hôtes valides par sous-réseau.
Calculez le masque de sous-réseau de la manière suivante :

1. Ajoutez 1 au nombre de sous-réseaux nécessaires et convertissez le résultat au format binaire.
2. Le nombre de bits obtenus, correspond au nombre de bits à ajouter au masque de sous-réseau par défaut.
   Insistons sur le fait, qu'il faut comptabiliser tous les bits à zéro à partir du premier 1. Si vous avez besoin de huit sous-réseaux, cela donne 1000 en binaire, soit quatre chiffres binaires, il faut ajouter 4 bits au masque de sous-réseau.
3. Placez le nombre de bits nécessaires au début de l'octet et complétez l'octet à huit chiffres avec des 0. 4
4. Convertissez le masque de sous-réseau au format décimal. Cette valeur remplacera le premier zéro du masque de sous-réseau.

Exemple :

Adresse IP (décimale)	168.20.0.0
Adresse IP	10101000 00010100 00010000 00000001
Masque de sous-réseau	11111111 11111111 00000000 00000000
L'ID de réseau	10101000 00010100 00000000 00000000

On a besoin de cinq sous-réseaux. D'après les étapes précédentes, la conversion donne 5 + 1 en binaire soit 0000110 ou plus simplement 110. Cela donne trois bits significatifs et un masque de 111.

Masque de sous-réseau	11111111 11111111 00000000 00000000
Le masque de sous réseau personnalisé donnera	11111111 11111111 11100000 00000000

Cette valeur en décimal vaut 255.255.224.0.

Définir les id de réseau à utiliser :

La méthode manuelle :
Il faut ajouter le nombre de bits nécessaire au masque de sous-réseau.
Il faut ensuite générer les IDs manuellement.

1. Recensez toutes les combinaisons binaires possibles des bits ajoutés au masque de sous-réseau par défaut.
2. Eliminez les combinaisons qui ne comprennent que des 0 ou que des 1 ; Elles ne sont pas valides. Une valeur ne contenant que des 1 représente une adresse de 1diffusion générale, et 0 signifie "uniquement ce réseau"
3. Convertissez les valeurs restantes en notation décimale. N'oubliez pas d'utiliser les 8 bits de l'octet pour la conversion décimale.
4. Ajoutez enfin chaque valeur à l'ID de réseau d'origine pour obtenir un ID de sous-réseau.

Exemple : La liste des combinaisons possibles est la suivante :
000 100
001 101
010 110
011 111

On écarte les valeurs 000 et 111. On convertit en décimal et on ajoute à la valeur d'origine.

Valeur binaire étendue	Valeur décimale	L'ID réseau
		168.20.0.0
00100000	32	168.20.32.0
01000000	64	168.20.64.0
01100000	96	168.20.96.0
10000000	128	168.20.128.0
10100000	160	168.20.160.0
11000000	192	168.20.192.0

Raccourci pour définir les ID de réseaux

La méthode suivante est plus rapide.

1. Une fois le nouveau masque de sous-réseau défini en fonction du nombre de sous-réseaux et d'ID d'hôtes voulus, Prenez la valeur binaire de l'octet définissant le masque de sous-réseaux.
2. Convertissez le bit 1 le plus à droite de cette valeur en décimal. C'est le bit de valeur 1 de rang le plus faible dans l'octet que vous avez calculé. Cette valeur décimale représente l'écart entre chaque numéro de sous-réseau, qu'on désigne par le terme delta.
3. Le nombre maximum d'ID de sous-réseaux utilisables est 2 à la puissance n moins 2 (2^n–2), n étant le nombre de bits nécessaire pour définir les sous-réseaux.
4. Ajoutez l'octet de valeur delta à l'iD de réseau d'origine pour obtenir le premier ID de sous-réseau.
5. Répetez l'étape 4 pour chaque ID de sous-réseau, en ajoutant chaque fois le delta.

Exemple :

Adresse IP (décimale)	168.20.0.0
Adresse IP	10101000 00010100 00010000 00000001
Masque de sous-réseau	11111111 11111111 00000000 00000000
L'ID de réseau	10101000 00010100 00000000 00000000

On a besoin de cinq sous-réseaux. D'après les étapes précédentes, la conversion donne 5 en binaire soit 0000101 ou plus simplement 101.

Masque de sous-réseau	11111111 11111111 00000000 00000000
Le masque de sous réseau personnalisé donnera	11111111 11111111 11100000 00000000

Le bit à droite convertit en décimal (00100000) donne 32. La valeur d'incrément est donc 32. Il y aura 2^3–2 = 6 sous-réseaux créés.

Les sous-réseaux qui sont créés sont :
168.20.0.0 plus 32 = 168.20.32.0
168.20.32.0 plus 32 = 168.20.64.0
168.20.64.0 plus 32 = 168.20.96.0
168.20.96.0 plus 32 = 168.20.128.0
168.20.128.0 plus 32 = 168.20.160.0
168.20.169.0 plus 32 = 168.20.192.0

4.3.5 La notion de suréseaux (CIDR)

Avec le système des classes A, les classes A et B ont été réduites à une portion congrue et les entreprises ce sont retrouvées avec des adresses de classe C.
Considérons une adresse de classe C, la 200.201.202.1.
Une adresse de classe C se voit attribuer automatiquement un masque de 255.255.255.0
L'identifiant réseau est le suivant : 200.201.202.0
Les machines composant le réseau sont les suivantes.
200.201.202.1
200.201.202.2
200.201.202.3
...
200.201.202.254
Soit 254 machines au total.
Supposons qu'il me faut un réseau unique de 518 machines.
Il me faut trois adresses de classe C (Plus de classe A ou B disponible) . 254 machines fournies par la première, 254 machines pour la seconde et 10 pour la troisième.
Elles pourraient être ventilées comme suit :
200.201.202.1
200.201.202.254
200.201.203.1
200.201.203.254
200.201.204.1
200.201.204.254
La machine 200.201.202.1 ne peut communiquer avec la machine 200.201.203.1 et la machine 200.201.204.1. Elles ne peuvent communiquer entre-elles car elles appartiennent à trois réseaux distincts. Cela provient du masque réseau qui est de 255.255.255.0.
Pour comprendre transformons l'adresse en binaire.

Adresse IP	1 byte	2 byte	3 byte	4 byte
202.201.202.1	11001000	11001001	11001010	00000001
202.201.202.254	11001000	11001001	11001010	11111110
202.201.203.1	11001000	11001001	11001011	00000001
202.201.203.254	11001000	11001001	11001011	11111110
202.201.204.1	11001000	11001001	11001100	00000001
202.201.204.254	11001000	11001001	11001100	11111110
Masque	11111111	11111111	11111111	00000000

C'est bien le masque qui fait apparaître des adresses distinctes. Réduisons la taille du masque de telle sorte que toutes les adresses aient le même identifiant réseau.

Adresse IP	1 byte	2 byte	3 byte	4 byte
202.201.202.1	11001000	11001001	**11001**010	00000001
202.201.202.254	11001000	11001001	**11001**010	11111110
202.201.203.1	11001000	11001001	**11001**011	00000001
202.201.203.254	11001000	11001001	**11001**011	11111110
202.201.204.1	11001000	11001001	**11001**100	00000001
202.201.204.254	11001000	11001001	**11001**100	11111110
Masque	11111111	11111111	**11111**000	00000000

Nous avons maintenant un seul réseau, le 200.201.200.0
Et son masque de surreseau est le suivant 255.255.248.0

Définition. *On parle de* ***surréseau*** *quand on groupe plusieurs adresses de classe C en un seul réseau.*

Définition. *Le terme* ***Classless Internet Domain Routing*** *est aussi employé car on n'utilise plus la classe de l'adresse pour déterminer son masque.*
La technique du Classless Internet Domain Routing (CIDR ou routage de domaine Internet sans class) permet de résumer un bloc d'adresses de classe C en une seule entrée de table de routage.

4.3.6 Structure d'un paquet IP

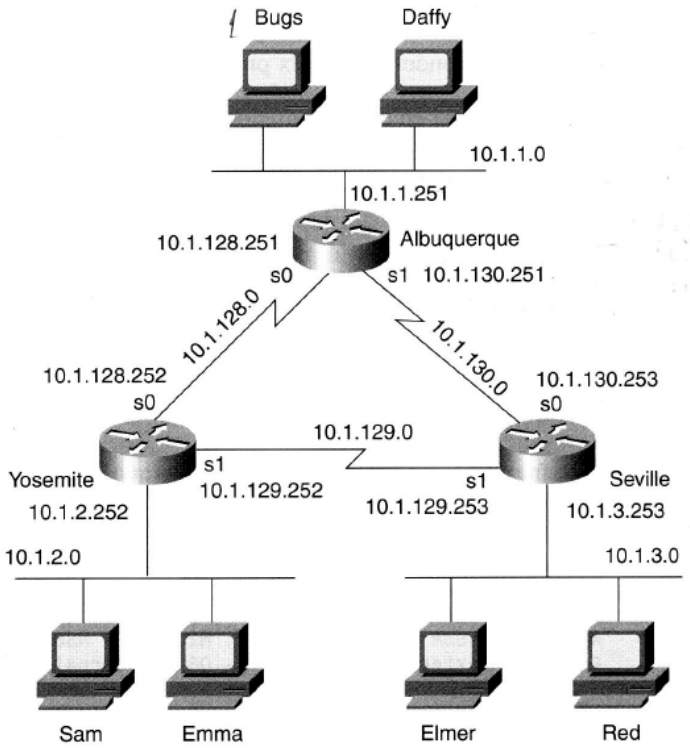
<table>
<tr><td colspan="6">32 bits</td></tr>
<tr><td>Version</td><td colspan="2">Longueur entête</td><td colspan="2">Type de service</td><td>Longueur totale</td></tr>
<tr><td colspan="4">Identification</td><td>Drap</td><td>Dep_fragment</td></tr>
<tr><td colspan="2">Protocole</td><td colspan="4">Total de contrôle d'en-tête</td></tr>
<tr><td colspan="6">Adresse source</td></tr>
<tr><td colspan="6">Adresse de destination</td></tr>
<tr><td colspan="6">Options</td></tr>
<tr><td colspan="6">Données</td></tr>
</table>

- Un datagramme IP est constitué de deux champs d'information : Un **champ en-tête** et un **champ données**, ce dernier constituant la charge utile du datagramme.
  L'en-tête comporte une partie fixe de 20 octets et une partie optionnelle de longueur variable.
  Le datagramme IP est transmit de la gauche vers la droite, le bit le plus à gauche du champ Version en premier.
- Le champ Version contient le numéro de version. La version actuelle est 4, notée Ipv4 ; Et la future IP est la version 6.
- Le champ **Lg_ent** indique sa longueur en mots de 32 bits.
- Le champ **Type** de service permet à un ordinateur d'indiquer au sous-réseau le type de service désiré.
- Le champ **Longueur totale** (16 bits) indique la longueur totale en octets du datagramme IP (le champ en-tête plus la charge utile). La taille maximale d'un datagramme IP est égale à 65535 octets.
- Le champ **Identification** est incrémenté de 1 chaque fois qu'un datagramme est envoyé. Si un datagramme doit être décomposé en plusieurs paquets appelés fragments, tous les fragments d'un même datagramme contiennent la même valeur.
- Le champ **Drapeau** qui indique si le paquet peut être fragmenté.
- **Dép_fragment** : précise la localisation ou le déplacement du fragment dans le datagramme courant. Tous les fragments, excepté le dernier du datagramme, doivent avoir des longueurs multiples de 8 octets, l'unité élémentaire du fragment.
- **Durée de vie** : est un compteur utilisé pour limiter la durée de vie des datagrammes. Il décompte le temps de séjour (en seconde) du datagramme dans le réseau avec une limite maximale de 255 secondes. En pratique il est décrémenté de un à chaque saut. Le passage du compteur à la valeur zéro déclenche la destruction du datagramme et l'émission d'un datagramme d'avertissement à l'ordinateur source concerné.
- Le champ **Protocole** lui indique par un numéro à quel protocole de transport le confier. Cela peut être TCP ou UDP, voire un autre protocole.
- Le champ **Total de contrôle d'en-tête** vérifie exclusivement la validité de l'en-tête. Sa fonction est la détection d'erreurs à l'intérieur des routeurs.
- Les champs **Adresse source** et **Adresse de destination** font chacun référence à un couple (numéro de réseau, numéro d'ordinateur).Ils contiennent chacun une IP.
- Le champ **Options** fut conçu pour offrir une extension aux évolutions du protocole IP afin de lui permettre de prendre en compte des informations et/ou des services non définis dans la version d'origine. Chaque option commence par un octet d'identification. Certaines options sont suivies par un champ **Longueur d'option**. Les champs Options ont une longueur multiple de 4.

4.3.7 Le routage statique

Définition. *Le **routage statique** se caractérise par le fait que les seules entrées de la table de routage sont simplement les adresses des réseaux auquel appartiennent les interfaces de la machine et que toute nouvelle entrée doit être configurée manuellement via l'opérateur.*

Le routage statique consiste en des commandes de configuration individuelles qui définissent des routes sur un routeur.
Un routeur ne peut transmettre des paquets que vers les sous-réseaux présents dans sa table de routage. Il connaît d'office les routes qui lui sont directement connectées, celles qui partent des interfaces dans un état « up » et « up ». En ajoutant des routes statiques, vous lui demandez d'acheminer des paquets vers des sous-réseaux qui ne lui sont pas directement reliés.



A partir de Albuquerque, la commande ping 10.1.128.2 fonctionne car Albuquerque possède une route vers le sous-réseau auquel cette adresse participe. Par contre la commande ping 10.1.2.252

Les commandes suivantes devraient être rajoutées a Albuquerque
Ip route 10.1.2.0 255.255.255.0 10.1.128.252
Ip route 10.1.3.0 255.255.255.0 10.1.130.253

4.4 Les algorithmes de routage dynamique

4.4.1 Le routage dynamique : définition

Définition. *On parle de routage dynamique lorsque un routeur diffusera à destination des autres routeurs ses tables de routage et écoute en permanence les diffusions éventuelles de création, de modification ou de confirmation qu'ils peuvent exploiter. Les diffusions entre routeurs se produisent généralement toutes les 30 secondes, que les tables de routage aient été modifiées ou non.*

4.4.2 Routage à vecteur de distance

4.4.2.1 Définition

Définition. *Avec les algorithmes de **routage par vecteur de distance**, chaque routeur maintient sa propre table de routage, c'est-à-dire un vecteur qui lui indique pour chaque destination, la meilleure distance vers chaque destination et la ligne à utiliser dans chaque cas. Il met régulièrement à jour sa table de routage avec les informations reçues des routeurs voisins.*
*Une des technique de routage par vecteur de distance, la plus utilisée est **RIP**.*

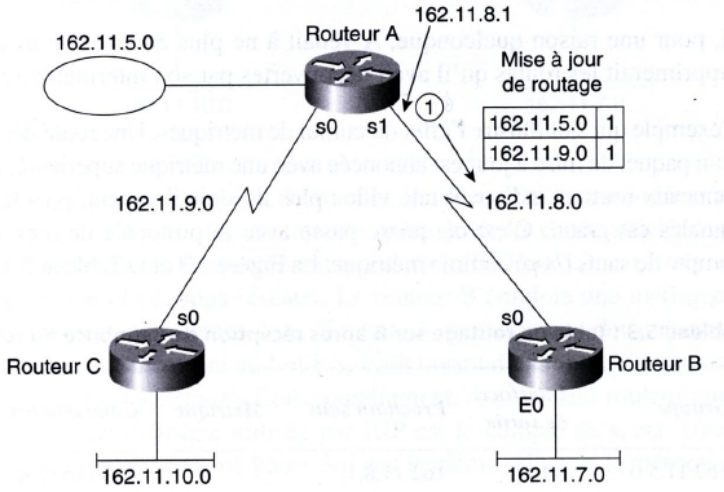
4.4.2.2 Les principes de base

Avec un protocole a vecteur de distance, un routeur annonce toutes les routes qu'il connaît sur toutes les interfaces. Les autres routeurs qui lui sont directement reliés, appelés routeurs voisins, reçoivent ces annonces et découvrent ainsi d'autres itinéraires.

4.4.2.3 Logique de fonctionnement

- Les routeurs ajoutent dans leur table de routage , les sous-réseaux qui leur sont directement connectés, même sans l'emploi d'un protocole de routage.
- Les routeurs envoient des mises à jour de routage sur leurs interfaces pour annoncer les routes qu'ils connaissent. Il s'agit des routes directement connectées et de celles qu'ils ont découvertes par l'intermédiaire d'autre routeurs.
- Les routeurs restent attentifs à la réception de mises à jour de la part de leurs voisins afin de prendre connaissance de l'existence de nouvelles routes.
- Les informations de routage incluent le numéro de sous-réseau et une métrique. La métrique permet de définir le niveau de qualité d'une route. Moins la valeur de métrique est élevée, meilleure est la route.
- Lorsque cela est possible, les routeurs emploient la diffusion broadcast ou multicast pour envoyer des mises à jour de routage. Avec l'emploi d'un paquet broadcast ou multicast, tous les voisins sur un LAN peuvent recevoir les mêmes informations de routage alors qu'un seul paquet a été émis.
- Si un routeur prend connaissance de plusieurs routes vers un même sous-réseau, il choisira le meilleur itinéraire en se fondant sur le métrique.
- Les routeurs envoient périodiquement des mises à jour complètes et s'attendent à recevoir aussi à intervalle régulier, des mises à jour de leurs voisins.
- Si un voisin n'envoie pas de mise à jour après le délai imparti, les routes précédemment découvertes par son intermédiaire sont supprimées de la table.

Schéma :



Voici la tabe de routage de B :

Réseau Masque : 255.255.255.0	Interface de sortie	Prochain Saut ou Gateway	Remarques
162.11.5.0	S0	162.11.8.1	Une des deux routes découvertes suite à l'annonce du routeur A
162.11.7.0	E0		Une route Directement Connectée
162.11.8.0	S0		Une roue Directement Connectée
162.11.9.0	S0	162.11.8.1	Une des deux roues découvertes suite à l'annonce du routeur A

On notera que si A n'envoie plus de mise à jour vers B. Les entrées correspondantes de la table de B seront supprimées.

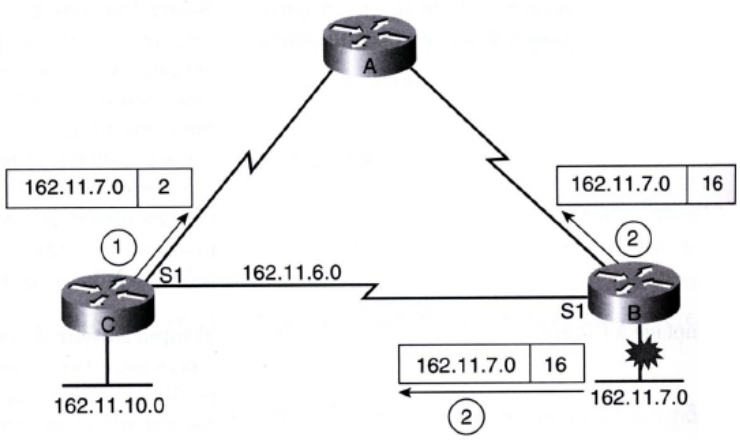
4.4.2.4 Les problèmes liés au vecteur de distance

Le routage à vecteur de distance fonctionne en théorie mais il s'accompagne d'un sérieux incovénient dans la pratique. Il ne réagit pas immédiatement aux changements du réseau. Il converge bien vers un réponse correcte mais trop lentement.

4.4.2.5 Les solutions

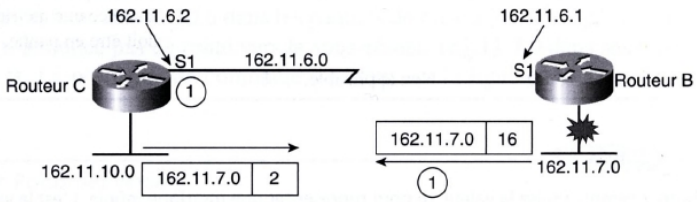
Le route poisoning :
Ceci se traduit littéralement par empoisonnement de route. Celle-ci intervient lorsqu'un routeur s'aperçoit qu'une route connectée n'est plus valide. Par exemple, un routeur détecte une ligne série défaillante et change l'état « up et up » en état « down et down ». Au lieu d'arrêter d'annoncer cette route, le protocole de routage qui emploie Route-Poisoning continue à la diffuser, mais avec une métrique très élevée signifiant une distance infinie.

Soit l'exemple ci-dessous, L'interface Ethernet du routeur B tombe en panne invalidant la route 162.11.7.0. Le routeur B annonce cette route avec une valeur infinie.



Le routeur C n'est pas encore informé de la panne et transmet la route 162.11.7.0 avec le métrique 2 vers A. Mais A recevant la route 162.11.7.0 aussi de B, sait grâce au métrique de 16 que cette route est invalide et la supprime. C reçoit finalement aussi la route 162.11.7.0 de B et supprime définitivement la route de sa table de routage.

Le split horizon :

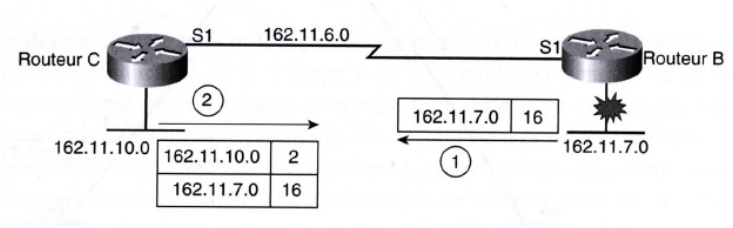


Le route Poisoning ne résoud malheureusement pas tout les problèmes.
Le problème est le suivant B reçoit la route suivante 162.11.7.0 de C avec la métrique 2.
B croit le réseau 162.11.7.0 est joignable par C mais il ne sait pas que C a eut cette information de lui-même.
Le problème se produit à nouveau lors de la mise à jour suivante. B anonce sa route avec un métrique de 3 et C annonce la route 162.11.7.0 avec un métrique de 15.
Et nous sommes repartit pour plusieurs tours ou le métrique de 162.11.7.0 va passer progressivement de 3 à 4,5,6 ... 16. On ne dépassera pas la valeur 16 car chaque protocole prévoit une valeur limite pour la représentation de l'infini.

Ce problème est connu sous le nom de **comptage à l'infini** (counting to infinity). Certains auteurs parlent du problème de la **valeur infinie**.
La solution est d'activer la fonction **split Horizon** (**Horizon éclaté**). On peut résumer cette fonction de la manière suivante :

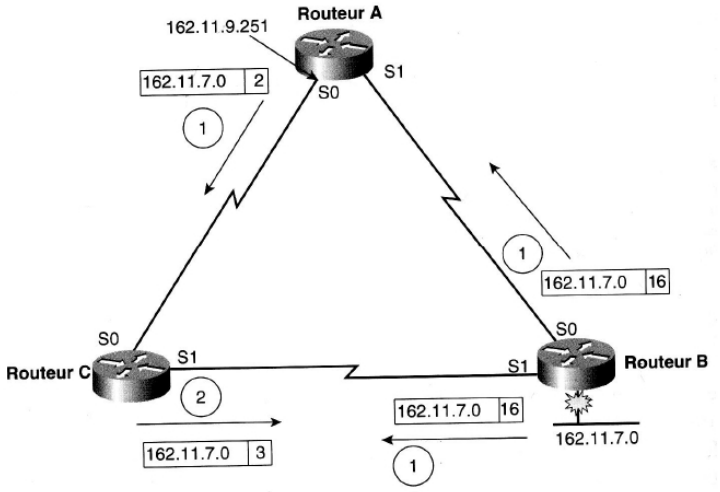
Définition. *Toutes les routes accessibles reçues à partir d'une certaine interface ne doivent pas être incluses dans une mise a jour sortant par cette même interface.*

Le split horizon avec Poison-reverse :
Lorsque le réseau est stable, le système fonctionne comme la Split-Horizon Simple. Mais lorsqu'un routeur reçoit une information de sous-reseau infinie, elle est recopiée sur toutes les routes y compris celle qui sont normalement interdites.



La figure ci-dessus montre que C a pris connaissance de la route de métrique infinie (valeur 16 pour RIP) vers le sous-réseau 162.11.7.0. Il ignore les règles de Split Horizon pour cette route et annonce le même sous-réseau à B avec une métrique infinie . L'emploi de Split-Horizon supprime le risque de comptage à l'infini , et l'ajout de Poison-Reverse garantit que les routeurs savent qu'une route est en panne.

Temporisateur Hold Down :
La fonction Split Horizon résout le problème de comptage à l'infini sur une seule liaison.
Ce problème peut se produire sur des réseaux redondants (comprenant plusieurs chemins vers un même sous-réseau), même si cette fonction est activée.
Dans ce cas,la fonction de **temporisation de retenue**, ou **Hold-Down**, remédie au problème.



La figure ci-dessus illustre une situation de comptage à l'infini non solutionnée par Split-Horizon mais par la fonction de retenue. Le sous-réseau 162.11.7.0 est de nouveau en panne et le routeur B annonce une route de métrique infinie vers ce sous-réseau aux routeurs A et C.
Malheureusement, le temporisateur du routeur A expire en même temps que celui de B et leurs mises à jour respectives arrivent en même temps.
C prend donc connaissance d'une route infinie par l'intermédiaire de B et d'une route de métrique 2 par l'intermédiaire de A.
Comme C doit prendre la plus courte il intègre donc la route en provenance de A.
Après les mises à jour (marquées d'un 1 dans la figure), routeur C pense qu'il possède une route valide vers 162.11.7.0 avec le routeur A pour intermédiaire.
Lors de la prochaine mise à jour, il n'annonce pas cette route à A via S0 a cause de la règle de split horizon mais à B avec un métrique de 3. Le routeur B croit de façon incorrecte que la route vers 162.11.7.0 existe par l'intermédiaire de C et l'annonce avec une métrique supérieure à 4.
Le problème de comptage à l'infini se produit même avec la fonction Split Horizon activée.

Définition. *Lorsqu'un routeur prend connaissance de l'indisponibilité d'une route vers un sous-réseau, il doit ignorer toute information concernant un chemin vers ce sous-réseau pendant une durée égale au temporisateur Hold-Down*

Avec ce temporisateur activé, le routeur C se retient de prendre en compte l'annonce du routeur A indiquant une métrique de 2, pendant la durée prévue par le temporisateur . Durant ce laps de temps, l'annonce avec métrique infinie émise par B et reçue par C est aussi reçue par A.
A peut ensuite la prendre en compte dans sa prochaine mise à jour et, conformément, annoncer une route de distance infinie vers le sous-réseau en panne.
Avec cette fonction de retenue, tous les routeurs ignorent les informations de route correcte vers un sous-réseau venant d'être signalé inaccessible, suffisamment longtemps pour que tous les routeurs reçoivent l'annonce de distance infinie.
Dans son principe, le temporisateur Hold-Down ne fait que demander aux routeurs de patienter un peu jusqu à ce que tous les routeurs prennent connaissance d'une panne, évitant ainsi la formation de boucles.
Il est de loin préférable d'attendre un peu plus longtemps la convergence afin d'éviter les problèmes provoqués par des paquets qui circulent en boucle.

4.4.3 Le routage par information d'état de lien

4.4.3.1 Le principe de fonctionnement

L'algorithme qui le remplace s'appelle **routage par informations d'état de lien (link state routing)**.
Dans le routage à vecteur de distance (ex : rip), un routeur n'envoie sa table de routage qu'a ses voisins immédiats. Dans le protocole à état de lien, tous les routeurs vont ici recevoir la table. Les routeurs auront ainsi une vue plus globale.

Le principe de fonctionnement est simple. Les actions que le routeur doit entreprendre sont les suivantes :

1. Découvrir ses voisins et apprendre leur adresse réseau.
2. Mesurer le temps d'acheminement vers ses voisins.
3. Construire un paquet spécial disant tout ce qu'il vient d'apprendre.
4. Envoyer le paquet vers tous les autres routeurs.
5. Calculer le chemin le plus court.

4.4.3.2 Découvrir ses voisins

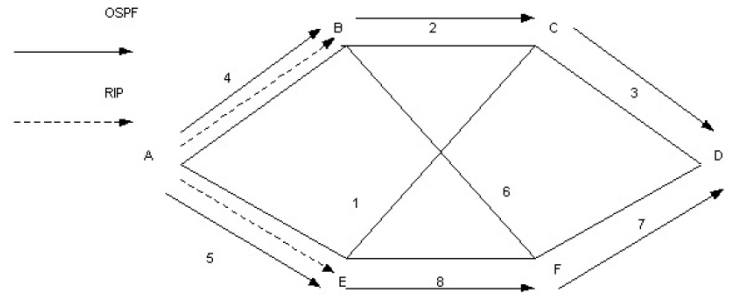
– Envoyer un paquet spécial hello sur ses lignes de sortie accompagné d'un point d'interrogation, et attendre la réponse.
– Les routeurs retournent leur nom et adresses qui doivent être uniques.
– Les LAN sont considérés comme des nœuds.

4.4.3.3 Mesurer le temps d'acheminement

– On transmet un paquet spécial ECHO vers le routeur voisin qui le retransmet
– On divise le temps obtenu par deux.
– On peut mesurer aussi la charge de la ligne en mesurant le temps d'émission depuis le placement dans la file et pas à l'émission du paquet.

4.4.3.4 Construire un paquet d'information d'état de lien

– Ces paquets sont construits à intervalles réguliers
– Exemples de paquets



A	
Séq	
Age	
B	4
E	5

B	
Séq	
Age	
A	4
C	2
F	6

C	
Séq	
Age	
B	2
D	3
E	1

D	
Séq	
Age	
C	3
F	7

E	
Séq	
Age	
A	5
C	1
F	8

F	
Séq	
Age	
B	6
D	7
E	8

4.4.3.5 Envoyer les paquets d'informations d'état de lien

Le mécanisme de distribution est le suivant :
– Utiliser l'inondation pour délivrer les paquets
– Chaque paquet à un numéro de séquence qui sert à éviter les paquets dupliqués ainsi que le numéro du routeur qu'il a émit.
– Tout nouveau paquet est retransmis sur les lignes de sortie.
– Tout paquet dupliqué est détruit.
– Tout paquet avec un numéro de séquence inférieur est détruit.

4.4.3.6 Les problèmes rencontrés

– Si un routeur tombe en panne, tous les paquets qu'il émettra seront rejetés.
– Modification accidentelle du numéro de séquence. Tous les paquets suivants sont détruits.

4.5 Quelques protocoles

4.5.1 IGRP : Interior Gateway Routing Protocol

Interior Gateway Routing Protocol (IGRP) est un protocole de routage de type distance-vector créé par Cisco et utilisé par les routeurs pour échanger leurs tables de routage dans un système autonome.
IGRP a été créé en partie pour remédier aux limitations de RIP quand il est utilisé dans de grands réseaux.
IGRP permet des métriques [1] multiples pour chaque route, en incluant la bande passante, la charge, le délai, MTU (Maximum Transmission Unit), et la fiabilité ; pour comparer 2 routes ces métriques sont combinés en un seul, en utilisant une formule ajustable.
Le nombre maximum de « hop » pour les paquets routés en IGRP est de 255 (la valeur infinie).
IGRP intègre le Trigger Update, le Hold Down et le Reverse Poisonning.
IGRP fait du **load-balancing** [2].

[1] la métrique est une distance qui sépare un routeur d'un réseau de destination. Elle peut correspondre au nombre de sauts IP nécessaires pour atteindre le réseau destination, comme dans RIP ; à un coût numérique qui dépend de la bande passante des liens franchis, comme dans OSPF ou à un vecteur, qui tient compte de la charge, du délai, du MTU, etc. comme dans EIGRP.
[2] Technique consistant à distribuer le trafic réseau sur plusieurs routes

4.5.2 EIGRP : Enhanced IGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) est un protocole de routage développé par Cisco à partir de leur protocole original IGRP. EIGRP est un protocole de routage hybride IP, avec une optimisation permettant de minimiser l'instabilité de routage due aussi bien au changement de topologie qu'à l'utilisation de la bande passante et la puissance du processeur du routeur.
Certaines de ces optimisations sont basées sur le Diffusing Update Algorithm (DUAL) développé par SRI, qui garantit l'absence de boucle. En particulier, DUAL évite les « sauts à l'infini » en les limitant à 224 et par conséquent les convergences sont plus rapides.
EIGRP utilise le VLSM (Variable Length Subnet Mask) et gère les CIDR (Classless Inter Domain Routing) c'est à dire le surréseau.

4.5.3 OSPF : Open Shortest Path First

OSPF (Open Shortest Path First) est un protocole de routage IP interne de type protocole à état de liens (link-state protocol) et qui offre une convergence très rapide.

4.5.4 BGP : Border Gateway Protocol

Border gateway protocol (BGP) est un protocole d'échange de route utilisé notamment sur le réseau Internet (routage des paquets sur des réseaux différents). Son objectif est d'échanger des réseaux (adresse IP + masque) avec ses voisins par le biais de sessions TCP.
C'est un protocol de type Exterior Gateway qui mémorise la route afin d'éviter le problème de la valeur infinie.

4.5.5 ACLs : Access Control Lists

Une ACL sur un pare-feu ou un routeur filtrant, est une liste d'adresses ou de ports autorisés ou interdits par le dispositif de filtrage.
Les Access Control List sont divisés en trois grandes catégories, l'ACL standard, l'ACL étendue et la nommée-étendue.
– l'ACL standard ne peut contrôler que deux ensembles : l'adresse IP source et une partie de l'adresse IP source, au moyen de masque générique
– l'ACL étendue peut contrôler l'adresse IP de destination, la partie de l'adresse de destination (masque générique), le type de protocole (TCP, UDP, IGRP, etc), le port source et de destination, les flux TCP, IP TOS (Type of service) ainsi que les priorité IP.
– l'ACL nommée-étendue est une ACL étendue à laquelle on a affecté un nom.
Les ACL sont différentes pour chaque port, pour chaque sens et pour chaque protocole et sont les seules à avoir accès au segment TCP.

4.5.6 ICMP : Internet Control Message Protocol

Internet Control Message Protocol est l'un des protocoles fondamentaux constituant la suite de protocoles Internet. Il est utilisé pour véhiculer des messages de contrôle et d'erreur pour cette suite de protocoles, par exemple lorsqu'un service ou un hôte est inaccessible.
ICMP se situe au même niveau que le protocole IP bien qu'il ne fournisse pas les primitives de service habituellement associées à un protocole de couche réseau. Son utilisation est habituellement transparente du point de vue des applications et des utilisateurs présents sur le réseau.

4.5.7 ARP : Adresse Resolution Protocol

L'Address resolution protocol (ARP, protocole de résolution d'adresse) est un protocole effectuant la traduction d'une adresse de protocole de couche réseau (typiquement une adresse IPv4) en une adresse ethernet (typiquement une adresse MAC), ou même de tout matériel de couche de liaison.

4.5.8 RARP : Revers ARP

RARP (pour Reverse ARP) permet à partir d'une adresse matérielle (adresse MAC) de déterminer l'adresse IP d'une machine. En résumé, RARP fait l'inverse de ARP.

4.6 Le VLAN : Virtual LAN

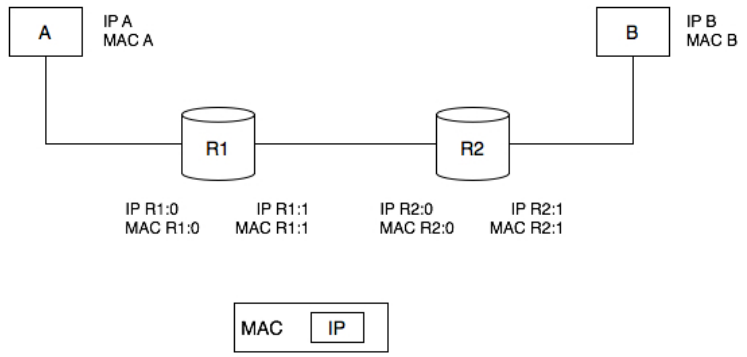
Un réseau virtuel, communément appelé VLAN (pour Virtual LAN), est un réseau informatique logique indépendant. De nombreux VLANs peuvent coexister sur un même commutateur réseau (switch).

Les intérets du VLAN :
- **Segmentation** : réduire la taille d'un domaine de broadcast
- **Flexibilité** : Possibilité de travailler au niveau 2 (couche liaison) (Adresse MAC) ou au niveau 3 (IP) : Les VLAN peuvent être configuré
  - soit sur base du port
  - soit sur base de l'IP
  - soit sur base de l'adresse MAC
  - soit sur base du numéro de port du transport = application
- **Sécurité** : permettre de créer un ensemble logique isolé pour améliorer la sécurité. Le seul moyen pour communiquer entre des machines appartenant à des VLANs différents est alors de passer par un routeur.

On peut avoir des switchs qui gèrent le VLAN ; ce sera alors le routeur qui décidera si les données peuvent passer d'un VLAN à un autre.

4.7 Adresse globale et adresse locale

Dans le cas d'une adresse globale, les adresses sont les mêmes de bout en bout (adresses IP).
Dans le cas d'une adresse locale, les adresses sont les mêmes sur le réseau mais changent de machine en machine (adresses MAC).



A veut envoyer des données à B :

source	IP A - MAC A	IP A - MAC R1 :1	IP A - MAC R2 :1
destination	IP B - MAC R1 :0	IP B - MAC R2 :0	IP B - MAC B

Note : Les routeurs désencapsules les adresses IP et les réencapsules.

Chapitre 5

La couche transport

5.1 Introduction

Le rôle de la couche transport est de permettre le transfert d'informations de la machine émettrice vers la machine réceptrice, de manière fiable et économique, indépendamment de la nature du ou des réseaux mis en place.

- La plupart du temps, les connexion transport utilisent une seule connexion réseau pour véhiculer les données. Or la connexion réseau n'utilise qu'une seule adresse logique. Il faut donc introduire la notion d'adresse transport (**TSAP**) pour que la couche transport puisse délivrer les segments à la bonne connexion transport.
- Toute communication entre entité de niveau transport met en oeuvre un port source et un port destination.
- Elle crée un canal virtuel qui dissimule les caractéristiques du réseau.
- Offre un service de type connecté et non connecté. Dans le cas de tcp/ip, c'est tcp pour le mode connecté et udp dans le cas du mode non connecté.
- Dans le cas de TCP, les messages sont aussi désignés segments.
- Offre un mécanisme de contrôle de flux de bout en bout dans le cas de tcp, c'est à dire qu'on vérifie si l'autre est saturé ou non)
- Offre un mécanisme d'acquittement dans le cas de tcp.
- Le mode non connecté offre un délai de réaction plus rapide mais sans garantie de fiabilité.

Lorsque l'on associe une adresse Ip et un numéro de port, on appelle ça un **socket**.

5.2 Présentation des protocoles TCP/UDP

5.2.1 Leur position dans le modèle TCP/IP

TCP et UDP forment la couche de transport de la pile TCP/IP. Ils se situent par rapport à IP de la manière suivante :

<table>
<tr><td>Processus 1</td><td>Processus 2</td><td>La couche application</td></tr>
<tr><td>TCP</td><td>UDP</td><td>La couhe transport (TSAP)</td></tr>
<tr><td colspan="2">IP</td><td>La couche réseau (NSAP)</td></tr>
<tr><td colspan="2">Interface Hardware
(la carte réseau)</td><td>La couche liaison de données (MAC)</td></tr>
</table>

TCP procure un service orienté connexion fiable.
UDP offre un service sans connexion, non fiable à base de datagramme.

TSAP = Transport Service Access Point
NSAP = Network Service Access Point

5.2.2 Comparaison entre ip, udp et tcp

Fonctionnalité	IP	UDP	TCP
Orienté connexion ?	Non	Non	Oui
Frontière des messages respectées ?	Oui	Oui	Non
Checksum des données ?	Non	Optionnel	Oui
Mécanisme d'ACK ?	Non	Optionnel	Oui
Timeout et réémission ?	Non	Non	Oui
Détection des duplicatas ?	Non	Non	Oui
Séquencement ? (remise dans l'ordre des datagrammes)	Non	Non	Oui
Contrôle de flux ?	Non	Non	Oui

La couche IP procure un service non fiable sans connexion pour TCP. C'est le module TCP qui contient la logique nécessaire pour un circuit virtuel fiable pour un processus utilisateur.

UDP procure seulement deux fonctionnalités qui ne sont pas offertes par IP : les numéros de ports et un checksum optionnel pour vérifier les contenus des datagrammes UDP.

5.3 Le protocole UDP

UDP (User Datagramme Protocol) est un protocole de transport en mode non connecté.
La structure du datagramme UDP est la suivante :

Port source	Port destination
Longueur UDP	Total de contrôle UDP
Data	

La longueur UDP comprend l'en-tête de 8 octets et les datas.

5.4 Le protocole TCP

5.4.1 La structure du datagramme TCP

<- 32 bits ->								
Port Source 1804								Port destination 80
Numéro de séquence								
Numéro d'accusé de réception								
Long En-tête TCP		URG	ACK	PSH	RST	SYN	FIN	Taille de fenêtre
Total de contrôle								Pointeur d'urgence
Options (0, 1 ou plusieurs mots de 32 bits)								
Données (optionnelles) get								

Format de l'en-tête TCP :
- Les champs Port Source et Port destination désignent les ports de l'application.
- Le champ Numéro de séquence indique le numéro du premier octet du segment dans le flux de données. Insistons sur le fait que TCP est orienté flux d' octet et non flux de messages.
- Le champ Numéro d'accusé de reception indique le prochain octet souhaité. Acquitte par la même occasion les Numéro-d'accusé-de-reception-1 octets.
- La longueur de l'en-tête TCP indique combien de mots de 32 bits contient l'en-tête. Puisque la longueur du champ Options est variable, celle de l'en-tête l'est aussi. En fait ce champ indique le point de départ des données dans le segment. I est exprimé en multiple de 32 octets. Exprime aussi la longueur de l'en-tête.

- Un champ de 6 bits n'est pas utilisé.
- On trouve un champ à 6 bits qui contient différents flags :

Champ	Signification
SYN	Synchronise les numéros de séquence. Ce flag est utilisé à l'ouverture d'une connexion.
URG	Vaut un si le pointeur d'urgence est uitlisé. Le pointeur d'urgence est un décalage en octets à partir du numéro de séquence courant que l'on utilise indiquer le dernier octet des données urgentes.
ACK	Est utilisé pour indiquer la validité du champ Numéro d'accusé de réception.
PSH	On demande à la couche transport destinataire de bien vouloir remettre les données à la couche application dès leur arrivée. En général, on accumule afin d'optimiser les performances.
RST	Pour réinitialiser un connexion devenue incohérente. A la réception de ce flag RST, le récepteur doit immédiatement terminer la connexion. Utilisé quand on ne sait pas réaliser une demande d'ouverture.
Fin	On utilise le bit Fin pour libérer une connexion. Il indique que l'émetteur n'a plus de données à transmettre mais qu'il peut continuer à en recevoir.

- Le champ Taille de fenêtre permet le contrôle de flux et indique combien d'octets l'émetteur peut transmettre après acquittement. On peut indiquer une taille de fenêtre nulle si le récepteur est submergé. C'est le récepteur qui fournit cette information à l'émetteur.
- Le champ Total de contrôle permet d'assurer une très grande fiabilité (CRC).
- Le fait de reprendre les adresses IP dans le total de contrôle viole le principe de neutralité des couches.
- Le champ option permet de spécifier plusieurs options.

5.4.2 La notion d'acquittement cumulé ou retardé, acquitement superposé

Exemple 1 : Considérons un émetteur et un récepteur qui s'échangent des données. Chaque donnée est acquitée.

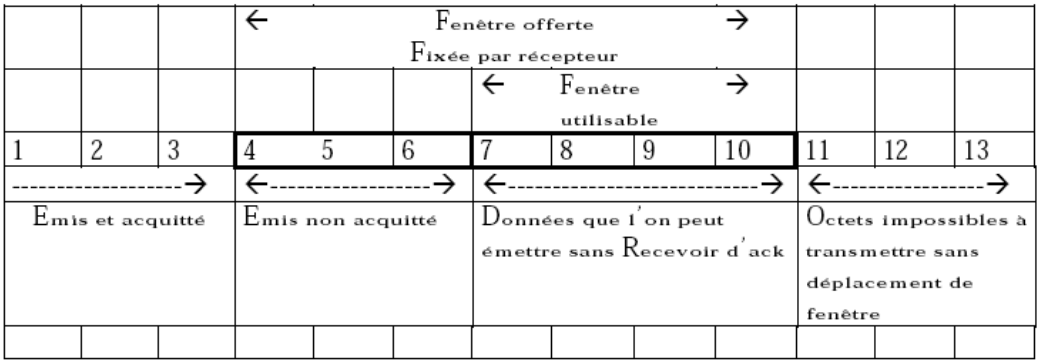
Emeteur		Récepteur
1	Envoi data 1 >>>	
	<<< ack 1	
2	Envoi data 2 >>>	
	<<< ack 2	
3	Envoi data 3 >>>	
	<<< ack 3	
4	Envoi data 4 >>>	
	<<< ack 4	

Exemple 2 : Considérons maintenant l'exemple suivant. Les données ne sont pas acquitée systématiquement à la réception.

Emeteur		Récepteur
1	Envoie data 1 >>>	
2	Envoie data 2 >>>	
3	Envoie data 3 >>>	
4	Envoie data 4 >>>	
	<<< Data 1, ack 4	

Les données sont transmises directement et les données sont acquittées par un **acquittement cumulé retardé**.
Un **acquittement cumulé** est un acquittement qui acquitte plusieurs données d'un coup. Les données 1 à 4 sont acquitées.
Un **acquittement retardé** est un acquittement qui n'est pas transmis directement à la réception de la donnée mais retardé jusqu'à ce que une trame de donnée est émise par le récepteur.
On parle d'**acquittement superposé aux donnée** (**piggyback**) quand l'acquittement est placé dans une trame de donnée émise par le récepteur.
Si après un certain laps de temps, aucune donnée n'est transmise par le récepteur, un acquittement seul sera envoyé par le récepteur.

5.4.3 Le concept de la fenêtre glissante


Fenêtre offerte
Fixée par récepteur
Fenêtre utilisable
1 2 3 4 5 6 7 8 9 10 11 12 13
Emis et acquitté
Emis non acquitté
Données que l'on peut émettre sans Recevoir d'ack
Octets impossibles à transmettre sans déplacement de fenêtre

Ce tableau représente un flux d'octets qui est numéroté de 1 à 13.
Le diagramme illustre la position courante de la fenêtre coté émetteur.

La **fenêtre offerte** par le récepteur à l'émetteur indique le nombre maximum d'octets que le récepteur peut recevoir. Dans le cas de tcp, cela indique la plage d'octets que l'émetteur peut émettre sans recevoir d'acquittement dans l'immédiat. Le transfert d'octets commence toujours à partir du dernier octet acquitté.

La **fenêtre utilisable** est la plage d'octets de la fenêtre offerte qui reste à émettre. Sa taille est toujours inférieure ou égale à la taille de la fenêtre offerte.
La fenêtre utilisable se ferme chaque fois qu'un octet est émis sans acquittement. Cela se traduit par le bord gauche qui se déplace vers la droite.

On dit la **fenêtre offerte** s'ouvre chaque fois que le récepteur acquitte les données reçues et traite l'information reçue, libérant son tampon. Cela se traduit par le bord droit qui se déplace vers la droite.

La **fenêtre glissante illustre** le fait que la fenêtre offerte à l'émetteur se déplace vers la droite chaque fois qu'un octet est acquitté et que la donnée est extraite de son tampon par le récepteur.

Dès que le bord gauche de la fenêtre offerte atteint le bord droit, on parle de **fenêtre zéro** et toute émission de donnée est stoppée.

La fenêtre offre un mécanisme de **contrôle de flux** : ans certaines circonstances, Le récepteur peut être incapable de traiter toutes les informations que l'émetteur lui envoie. Cela se traduira par un remplissage progressif des tampons du récepteur. Pour éviter tout débordement, le récepteur réduira progressivement la taille de la fenêtre offerte. Si le récepteur transmet une taille de fenêtre zéro, toute émission sera stoppée.

5.4.4 L'ouverture de connexion

5.4.4.1 Le problème de l'ouverture des connexions

A priori, cela semble simple. Il suffirait d'envoyer un paquet de demande de connexion au destinataire et d'attendre la réponse. Malheureusement, le réseau peut perdre, stocker ou dupliquer les paquets.
Scénario simple : suite à une congestion, les accusés de réception n'arrivent pas. Cela entraîne suite à un timeout l'émission de plusieurs paquets CONNECTION REQUEST. Ces paquets arrive finalement à destination entraînant l'ouverture de plusieurs connections. C'est gênant surtout dans le cas de transactions bancaires.
Une solution simple et efficace est l'**initialisation en trois étapes**.

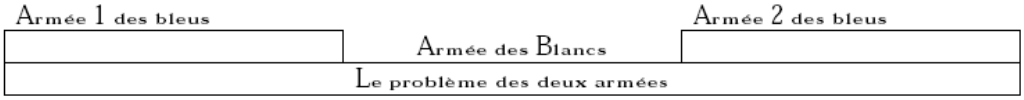
5.4.4.2 L'initialisation en trois étapes (Three ways handshake)

CONNECTION REQUEST X >>>	
	<<< CONNECTION ACCEPTED X,Y
CONNECTION ACCEPTED Y >>>	

- Chaque extrémité utilise une référence qui lui est propre.
- L'émetteur envoie un requête CONNECTION REQUEST contenant une référence X.
- Le récepteur confirme en envoyant une CONNECTION ACCEPTED qui acquitte la référence X et sa propre référence Y.
- Pour finir l'émetteur confirme au récepteur en envoyant un CONNECTION ACCEPTED avec sa référence X et l'acquittement de la référence Y.
- Si le récepteur reçoit une demande de connexion dupliquée il acquittera et l 'émetteur se rendra compte qu'il reçoit un acquittement en double puisqu'il reçoit deux fois la référence X.

5.4.5 La fermeture de connexion

5.4.5.1 Le problème des deux armées

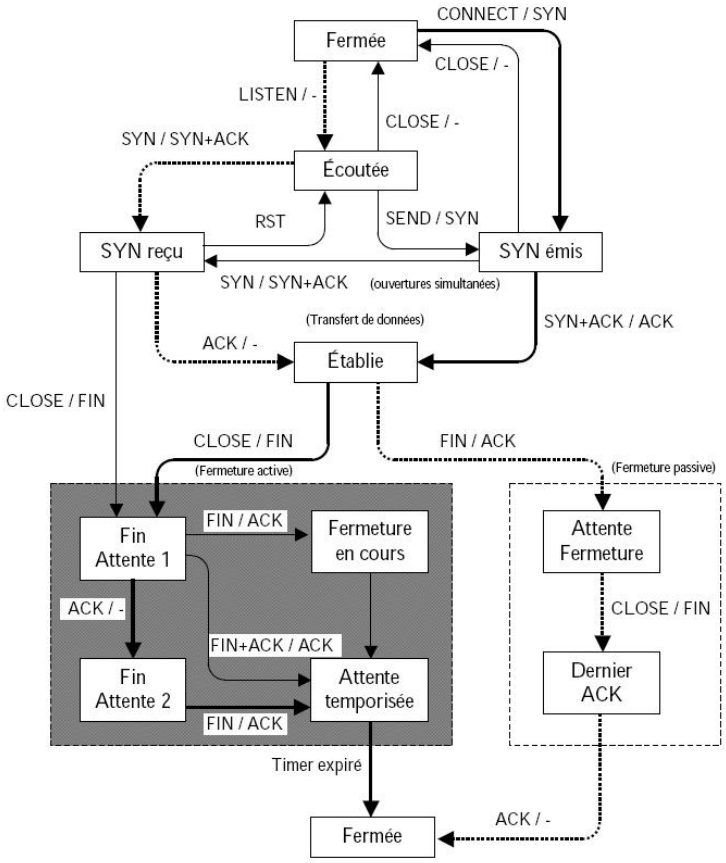


- Dans ce cas de figure, nous avons deux armées en présence. La blanche se situe au fond de la vallée et elle est encerclée par la troupe bleue qui a ses forces disposées en deux formations sur les collines qui surplombent la valée.
- La troupe bleue souhaite attaquer la troupe blanche. Mais pour réussir son attaque, il faudrait que les deux formations qui la compose, attaquent en même temps.
- Pour parvenir à cet objectif, La troupe de gauche envoie un messager à la troupe de droite. Ce messager passe par la vallée et du fait de la troupe ennemie, on n'est pas certain de son arrivée à destination. On peut multiplier les échanges de messagers à l'infini, rien ne garantit que le dernier messager arrive à destination.
- En d'autres termes, quand une troupe lancera son attaque à l'heure indiquée par le billet transmit par le messager, rien ne lui garantit que la formation située sur l'autre colline fera de même (le messager n'est pas arrivé à bon port).
- En réseau, la problématique est la même. Si une extrémité initie la déconnexion rien ne garantit que l'autre extrémité fera de même, le paquet transportant la demande de déconnexion peut se perdre.

5.4.5.2 L'approche TCP

- Pour libérer une connexion, chaque extrémité envoie un segment TCP avec le bit FIN positionné à 1. Ceci signifie qu'elle n'a plus de données à transmettre.
- Attention quand une entité ferme, elle peut continuer à recevoir des datas.
- Ce n'est que quand il y'a acquittement que la connexion est fermée.
- Il faut quatre segments pour fermer une connexion. Un FIN et un ACK dans chaque sens.
  Les étapes 2 et 3 peuvent cependant être regroupées en une seule. Ce qui réduit le nombre de segments échangés à trois.
- L'envoi du FIN est déclenché par la primitive close dans le programme émetteur ou récepteur.
- Pour éviter le problème des deux armées, on utilise un temporisateur. Si la confirmation n'est pas arrivée, on ferme la connexion unilatéralement

5.4.6 La machine d'états TCP



Etat	Description
Les états intervenant dans le processus d'établissement de la connexion	
Fermée	Les seules opérations permises sont alors une demande d'ouverture soit passive (passage à l'état Ecoutée), soit active correspondant à l'envoi d'un segment avec indicateur SYN (elle passe à l'état SYN émis)
Ecoutée	L'extrémité peut recevoir une demande de connexion active (segment avec l'indicateur SYN entraînant son passage à l'état SYN reçu) avec envoi de SYN et de ACK, soit faire elle-même une demande de connexion active avec une autre extrémité (entraînant son passage à l'état SYN émis)
SYN émis	L'extrémité qui a donc préalablement transmis une demande de synchronisation peut soit passer à l'état SYN reçu si elle reçoit une demande analogue qu'elle acquitte aussi (indicateur ACK positionné), soit passer à l'état Établie si elle reçoit à la fois une demande de synchronisation et un acquittement de sa demande antérieure (réception d'un segment avec les indicateurs SYN et ACK)
SYN reçu	L'extrémité a émis et reçu une demande de synchronisation. L'extrémité peut soit recevoir l'acquittement de sa demande de synchronisation (à sa réception par un segment avec l'indicateur ACK, elle passera à l'état Établie), soit transmettre un avis de fin de connexion (segment avec l'indicateur CLOSE/FIN entraînant son passage à l'état Fin attente 1). Cela peut se produire si le programme se termine.

La connexion est établie	
Établie	Il correspond au fait qu'une connexion a été effectivement établie. L'extrémité peut alors recevoir et émettre des segments de données ou entrer dans le processus de déconnexion. Elle quitte cet état soit si elle reçoit un avis de fermeture de connexion (entraînant son passage à l'état Attente Fermeture), soit si elle transmet elle-même un tel avis (entraînant son passage à l'état Fin attente 1).
Les états intervenant dans le processus de déconnexion initié par l'extrémité elle-même	
Fin Attente 1	L'extrémité a donc transmis un segment avec l'indicateur FIN. Elle peut alors recevoir un segment d'acquittement (entraînant son passage à l'état Fin attente 2 sans action particulière), soit recevoir un avis de fin de connexion (segment avec l'indicateur FIN/ACK qu'elle acquitte en passant à l'état Fermeture en cours)
Fin attente 2	L'extrémité a transmis un segment avec l'indicateur FIN qui a été acquitté. Elle attend alors un segment avec l'indicateur FIN qu'elle acquittera à sa réception en passant à l'état Attente temporisée.
Fermeture en cours	L'extrémité a transmis et reçu un segment de fin de connexion (indicateur FIN) qu'elle a acquitté. Elle attend l'acquittement de son segment de fin de connexion. A l'arrivée de celui-ci, elle passera à l'état Attente temporisée sans action spécifique.
Attente temporisée	La connexion est effectivement fermée. On entre dans un état pour une durée de 2*MSL où MSL est la durée de vie maximale estimée d'un segment (Maximal Segment Lifetime). Cet état empêche l'utilisation d'un port local pour une nouvelle connexiontant que ce numéro fait partie d'une paire de sockets qui est dans une attente 2MSL..
Les états intervenant dans le processus de déconexion initié par l'autre extrémité (celle qui subit la demande de déconnexion	
Attente Fermeture	L'extrémité a reçu une demande de fin de connexion (segment avec l'indicateur FIN) qu'elle a acquittée (segment avec indicateur ACK). Elle reste dans cet état jusqu'à ce qu'elle envoie une demande de fin de connexion (segment avec indicateur FIN entraînant son passage à l'état Dernier ACK).
Dernier ACK	L'extrémité a envoyé son avis de terminaison (segment avec indicateur FIN), a reçu celui de l'autre extrémité et l'a acquitté. Elle attend la réception de l'accusé de réception de sa demande de fin de connexion.
Fermée	La connexion est effectivement fermée.

5.4.7 La gestion des temporisateurs

TCP maintient 7 timer pendant une connexion dont voici la liste :

1. Un **timer d'établissement** de connexion démarre quand un segment SYN est envoyé pour établir une nouvelle connexion.
2. Un **timer de retransmission** est déclenché quand TCP envoie des données. Si ce timer se déclenche, cela veut dire que la donnée n'a pas été acquitée et TCP retransmet ses données.
3. Un **timer d'acquittement Retardé** est prévu. A chaque réception de données, ce timer est démarré. Si après 200 ms de temps, il n'y a pas de segment de données qui part dans l'autre sens, un segment avec des données factice est automatiquement émis avec cet acquittement. Ce mécanisme évite l'envoi de trames factices rien que pour transmettre des ACK. Cela évite de gaspiller de la bande passante.
4. Un **timer de persistance** est déclenché quand l'autre extrémité signale une fenêtre de taille 0, qui empêchera TCP d'envoyer des données.
5. Le **keepalive timer** peut être fixé par le processus en utilisant l'option SO_KEEPALIVE sur la socket. Si la connexion est inactive pour deux heures, ce timer expire et un segment spécial (une sonde) est envoyé à l'autre extrémité pour le forcer à répondre. Si la réponse attendue est reçue, TCP sait que l'autre extrémité est toujours là et TCP ne va pas la tester à nouveau sauf si la connexion est de nouveau inactive pour deux heures. Si aucune réponse n'est reçue après un nombre fixé d'envois de sondes keepalive, TCP suppose que la connexion est rompue.
6. Le **FIN_WAIT_2** timer est déclenché quand on passe de l'état FIN_WAIT_1 à l'état FIN_WAIT_2 et la connexion ne peut plus recevoir aucune donnée.
7. Un **TIME_WAIT timer**, souvent appelé le timer 2MSL.

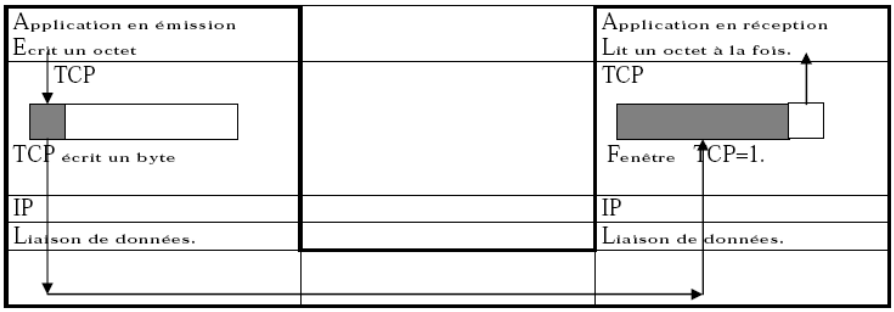
5.4.8 Les optimisations internets

5.4.8.1 L'algorithme de Nagle

L'algorithme de Nagle, quand une application envoie octet par octet, on envoie le premier octet et on stocke tout le reste. Le reste sera envoyé quand le premier octet est acquitté. Puis on envoie, dans un segment TCP, tous les caractères accumulés, et on recommence à stocker jusqu'à ce que tous les octets soient acquittés. Si l'utilisateur saisit rapidement et que le réseau est lent, il peut y avoir un grand nombre d'octets dans chaque segment, ce qui diminue fortement la largeur de la bande utilisée. L'algorithme de Nagle permet, en outre, d'envoyer un nouveau paquet s'il y a eu assez de données pour remplir la moitié de la fenêtre ou si l'on atteint la taille maximale de segment.

5.4.8.2 Le syndrome de la fenêtre stupide

Ce problème survient lorsqu'on passe des donénes à l'entité TCP émettrice par grands blocs, mais que côté récepteur, une application interactive les lits octets par octets.



Au départ, le tampon mémoire TCP côté récepteur est plein et l'émetteur le sait (c'est à dire qu'il a une fenêtre de taille 0). Puis l'application interactive lit un caractère en provenace du flux TCP. Cette action satisfait pleinement le récepteur TCP qui envoie donc à l'émetteur une indication d'actualisation de fenêtre pour qu'on lui envoie un octent. L'émetteur se sent obligé d'envoyer l'octet suivant. Le tampon mémoire est à nouveau plein et le récepteur acquitte le segment d'un octet mais positionne la fenêtre à 0. Et ainsi de suite ...

La **solution de Clark** consiste à empêcher le récepteur d'envoyer une indication d'actualisation de fenêtre juste pour un octet : on l'oblige à attendre d'avoir un espace disponible d'une taille décente avant de l'annoncer. En pratique, le récepteur ne doit pas envoyer une indication d'actualisation de fenêtre tant qu'il n'a pas atteint la taille maximale de segment qu'il avait obtenue lors de l'établissement de la connexion ou que son tampon mémoire est à moitié vide.

5.4.9 Le contrôle de la congestion TCP

Quand la charge est plus importante que ce qu'on est en mesure de gérer, il se produit une congestion.

En théorie, on peut traiter la congestion par la loi de conservation des paquets. L'idée est de ne pas injecter un nouveau paquet dans le réseau tant qu'un ancien subsiste. TCP essaie d'atteindre cet objectif en manipulant dynamiquement la taille de fenêtre.

Le premier stade de la gestion de congestion, c'est sa détection. Lorsqu'un temporisateur expire, on peut être sur qu'une congestion s'est produite car les grandes artères sur internet sont en fibre optique et par conséquent les erreurs dues aux erreurs de transmissions sont devenues rares.

La solution adoptée sur internet repose sur le fait qqu'il existe deux problèmes potentiels (capacité du réseau et capacité du récepteur) que l'on traite séparément. Chaque émetteur gère donc deux fenêtre : la fenêtre que le récepteur a accordée et la **fenêtre de congestion**. Chacune de ces fenêtres reflète le nombre d'octets que l'émetteur peut transmettre. Le nombre d'octets envoyés doit donc correspondre au minimum de ces deux fenêtres. La fenêtre réellement utilisée correspond au minimum de ce qui convient à l'émetteur et au récepteur. Si le récepteur dit "Envoyez 8Ko", mais que le récepteur sait qu'un envoie

de plus de 4Ko d'un coup peut engorger le réseau, il n'envoie que 4Ko. Réciproquement, si le récepteur dit "Envoyez 8Ko", alors que l'émetteur sait que tout envoie de moins de 32Ko passera sans problème, alors il envoie 8Ko.

Algorithme du démarrage lent (slow start) :
Au départ la fenêtre de congestion est initialisée au maximum de la taille de segment utilisée. Si l'acquittement arrive avant l'expiration du temporisateur, on ajoute à la taille de la fenêtre de congestion un segment. La règle générale est quand la fenêtre de congestion atteint n segments et que les n segments sont acquittés dans le temps impartit, la fenêtre est augmentée du nombre d'octets correspondant au n segments. Cela continue de grandir tant que l'on n'a pas atteint la limite de la fenêtre du récepteur ou qu'un temporisateur expire.

Pour la gestion des congestions, Internet utilise en plus, la notion de seuil d'évitement de congestion (threshold) de valeur initiale de 64Ko. Quand la fenêtre de congestion dépasse ce seuil, on croit de manière linéaire (ajout d'un seul segment au lieu du nombre de segments acquittés). Si un temporisateur expire, on redimensionne la taille de ce seuil d'évitement de congestion à la moitié et la fenêtre de congestion est réinitialisée à la taille maximum de segment.

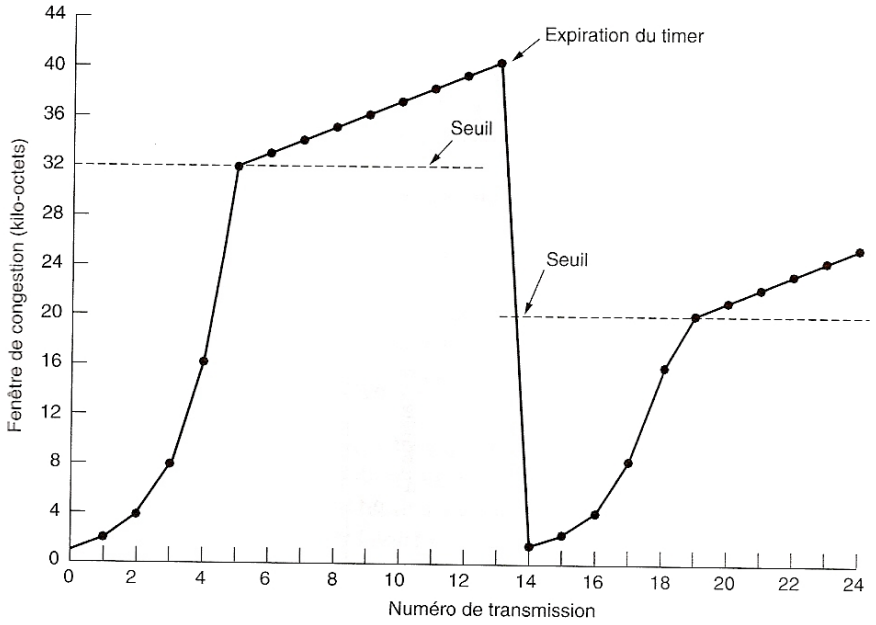


Table des matières

1 Terminologie et modèles de référence **1**
1.1 Définitions de base . . . 1
1.2 Les critères de classement des réseaux . . . 1
1.2.1 La technique de transmission . . . 1
1.2.1.1 La diffusion (Broadcast) . . . 1
1.2.1.2 Les réseaux point à point . . . 2
1.2.2 La taille du réseau . . . 3
1.2.2.1 LAN (Local Area Network) . . . 3
1.2.3 MAN (Metropolitan Area Network) . . . 4
1.2.4 WAN (Wide Area Network) . . . 4
1.2.5 Internet . . . 5
1.2.6 Le type de commutation . . . 5
1.2.6.1 La commutation de circuit . . . 5
1.2.6.2 Le mode datagramme . . . 6
1.2.6.3 Le mode virtuel . . . 7
1.3 Logigiel Réseau . . . 8
1.3.1 Principe d'une architecture en couche . . . 8
1.3.2 Hiérarchies de protocoles . . . 8
1.3.3 Protocoles/services en mode connecté/déconnecté . . . 9
1.3.3.1 Protocole en mode connexion . . . 9
1.3.3.2 Protocole déconnecté ou sans connexion . . . 9
1.4 Les modèles et normes de référence . . . 10
1.4.1 Le modèle de référence OSI (Open System Interface) . . . 10
1.4.2 Le modèle TCP/IP . . . 10
1.4.3 Le modèle ATM . . . 11

2 La couche physique : les signaux, cablages et interfaces **12**
2.1 Couche physique . . . 12
2.2 Distinction entre la transmission analogique et digitale . . . 12
2.2.1 La transmission analogique . . . 12
2.2.2 La transmission digitale ou numérique . . . 13
2.2.3 Conversion des signaux . . . 13
2.3 Bases théoriques de la transmission de données . . . 13
2.3.1 Représentation du courant électrique (d'un signal périodique) . . . 13
2.3.2 Décomposition en série de Fourrier . . . 14
2.3.3 La définition du décibel . . . 14
2.3.4 Définition de la bande passante et de la fréquence de coupure . . . 14
2.3.5 Influence du débit sur la transmission des harmoniques . . . 14
2.3.6 Débit maximum théorique d'un canal de transmission . . . 15
2.3.7 Débit maximum pratique d'un canal de transmission . . . 15
2.4 Les modems . . . 16
2.4.1 Le principe . . . 16
2.4.2 Les techniques de modulation . . . 16
2.4.2.1 Représentation d'un signal électrique . . . 16
2.4.2.2 Constellation diagramme . . . 17
2.5 Les médias de transmission . . . 18
2.5.1 Le câble électrique à paires torsadées . . . 18

2.5.2 Le câble coaxial bande de base . . . 19
2.5.3 La fibre optique . . . 20
2.6 Le multiplexage . . . 25
2.6.1 Le principe du multiplexage . . . 25
2.6.2 Le multiplexage fréquentiel . . . 26
2.6.3 Le multiplexage temporel . . . 26
2.7 Le wireless . . . 27

3 La couche liaison de données : Les connexions point à point, les réseaux 28
3.1 La couche Hote Réseau . . . 28
3.2 La couche Trame ou Liaison de données (Data Link Layer) . . . 29
3.3 Objectifs de la couche liaison de données . . . 30
3.3.1 Les services offerts à la couche réseau . . . 30
3.3.1.1 Le service sans connexion et sans accusé de réception . . . 30
3.3.1.2 Le service sans connexion et avec accusé de réception . . . 30
3.3.1.3 Le service orienté connexion et avec accusé de réception . . . 30
3.3.2 La notion de trames . . . 30
3.3.2.1 Remarques générales . . . 30
3.3.2.2 Les types de découpages en trames . . . 30
3.3.3 Le contrôle d'erreur . . . 31
3.3.4 Le contrôle de flux . . . 31
3.4 Détection et correction des erreurs . . . 31
3.4.1 Les codes correcteurs d'erreurs . . . 31
3.4.2 Les codes détecteurs d'erreurs . . . 32
3.5 La couche liaison dans les lignes point à point . . . 32
3.5.1 Les types de lignes point à point . . . 32
3.5.2 Le protocole PPP . . . 32
3.6 La couche liaison et les réseaux de type diffusions
MAC : La sous couche de contrôle d'accès au canal . . . 33
3.6.1 Introduction . . . 33
3.6.2 La sous couche MAC sous Ethernet . . . 33
3.6.2.1 CSMA/CD ou CSMA avec détection des collisions . . . 33
3.6.2.2 L'algorithme de backoff . . . 34
3.7 La norme IEEE 802.3 et réseau Ethernet . . . 36
3.7.1 Les réseaux commutés . . . 36
3.7.1.1 introduction . . . 36
3.7.1.2 Décision de transmission ou filtrage . . . 36
3.7.1.3 La découverte d'adresses . . . 37
3.7.1.4 Acheminement du traffic unicast à destination inconnue et du trafffic broadcast . . . 37
3.7.1.5 Synthèse logique de transmission d'un commutateur . . . 37
3.7.2 Les modes de retransmission interne des trames . . . 37
3.7.2.1 La méthode Store and Forward . . . 37
3.7.2.2 La méthode Cut and Through . . . 37
3.7.2.3 La méthode Fragment - Free . . . 38
3.7.3 L'algorithme du spanning tree (arbre en expansion) ou STP . . . 38
3.7.3.1 Le problème des boucles . . . 38
3.7.3.2 Présentation du Spanning Tree Protocol . . . 38

4 La couche réseau, le routage 39
4.1 Introduction . . . 39
4.1.1 La couche réseau (Network Layer) : ses fonctions . . . 39
4.1.2 Structure d'un paquet . . . 40
4.2 Généralités sur la couche réseau . . . 40
4.2.1 Evolution de la couche réseau . . . 40
4.2.1.1 La ligne louée . . . 40
4.2.1.2 Commutation de circuits . . . 40
4.2.1.3 Commutation de paquets . . . 41
4.3 La couche réseau dans internet . . . 41

4.3.1 Internet, qu'est-ce que c'est ? . . . 41
4.3.2 Les adresses IP . . . 42
4.3.2.1 Les fonctions de l'adresse IP . . . 42
4.3.2.2 Le rôle du routeur . . . 42
4.3.2.3 Le routeur vs hub vs switch . . . 42
4.3.2.4 La structuration de l'adresse ip . . . 42
4.3.2.5 Les classes d'adresses . . . 43
4.3.2.6 Les capacités des adresses . . . 43
4.3.2.7 L'étendue des adresses IP . . . 43
4.3.2.8 Comment attribuer des ip à des pc . . . 43
4.3.2.9 Les adresses réservées . . . 44
4.3.3 Les adresses de réseau publique/privé . . . 44
4.3.3.1 Les adresses publiques . . . 44
4.3.3.2 Les adresses privées . . . 44
4.3.4 Les sous-réseaux . . . 44
4.3.4.1 La problématique . . . 44
4.3.4.2 La solution . . . 45
4.3.4.3 La démarche de créer des sous-réseaux . . . 45
4.3.5 La notion de suréseaux (CIDR) . . . 48
4.3.6 Structure d'un paquet IP . . . 49
4.3.7 Le routage statique . . . 50
4.4 Les algorithmes de routage dynamique . . . 51
4.4.1 Le routage dynamique : définition . . . 51
4.4.2 Routage à vecteur de distance . . . 51
4.4.2.1 Définition . . . 51
4.4.2.2 Les principes de base . . . 51
4.4.2.3 Logique de fonctionnement . . . 51
4.4.2.4 Les problèmes liés au vecteur de distance . . . 52
4.4.2.5 Les solutions . . . 53
4.4.3 Le routage par information d'état de lien . . . 55
4.4.3.1 Le principe de fonctionnement . . . 55
4.4.3.2 Découvrir ses voisins . . . 55
4.4.3.3 Mesurer le temps d'acheminement . . . 55
4.4.3.4 Construire un paquet d'information d'état de lien . . . 56
4.4.3.5 Envoyer les paquets d'informations d'état de lien . . . 56
4.4.3.6 Les problèmes rencontrés . . . 56
4.5 Quelques protocoles . . . 56
4.5.1 IGRP : Interior Gateway Routing Protocol . . . 56
4.5.2 EIGRP : Enhanced IGRP . . . 57
4.5.3 OSPF : Open Shortest Path First . . . 57
4.5.4 BGP : Border Gateway Protocol . . . 57
4.5.5 ACLs : Access Control Lists . . . 57
4.5.6 ICMP : Internet Control Message Protocol . . . 57
4.5.7 ARP : Adresse Resolution Protocol . . . 57
4.5.8 RARP : Revers ARP . . . 57
4.6 Le VLAN : Virtual LAN . . . 58
4.7 Adresse globale et adresse locale . . . 58

5 La couche transport **59**
5.1 Introduction . . . 59
5.2 Présentation des protocoles TCP/UDP . . . 59
5.2.1 Leur position dans le modèle TCP/IP . . . 59
5.2.2 Comparaison entre ip, udp et tcp . . . 60
5.3 Le protocole UDP . . . 60
5.4 Le protocole TCP . . . 60
5.4.1 La structure du datagramme TCP . . . 60
5.4.2 La notion d'acquittement cumulé ou retardé, acquitement superposé . . . 61
5.4.3 Le concept de la fenêtre glissante . . . 62

5.4.4 L'ouverture de connexion 62
5.4.4.1 Le problème de l'ouverture des connexions 62
5.4.4.2 L'initialisation en trois étapes (Three ways handshake) 63
5.4.5 La fermeture de connexion 63
5.4.5.1 Le problème des deux armées 63
5.4.5.2 L'approche TCP 63
5.4.6 La machine d'états TCP 64
5.4.7 La gestion des temporisateurs 65
5.4.8 Les optimisations internets 66
5.4.8.1 L'algorithme de Nagle 66
5.4.8.2 Le syndrome de la fenêtre stupide 66
5.4.9 Le contrôle de la congestion TCP 66